DRAFT
NIST Special Publication 800-79-1

Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)

Dennis Bailey
Ramaswamy Chandramouli
Nabil Ghadiali
Dennis Branstad

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director & Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) stimulates U.S. economic growth and industrial competitiveness through technical leadership and collaborative research in critical infrastructure technology, including tests, test methods, reference data, and forward-looking standards, to advance the development and productive use of information technology. To overcome barriers to usability, scalability, interoperability, and security in information systems and networks, ITL programs focus on a broad range of networking, security, and advanced information technologies, as well as the mathematical, statistical, and computational sciences. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority, Usage, and Revisions

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under Homeland Security Presidential Directive 12, signed August 27, 2004.

NIST is responsible for developing standards and guidelines, including specifying minimum requirements, for providing adequate information security for all organizational operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This document has been prepared for use by Federal agencies but it also may be used by non-governmental organizations on a voluntary basis. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. This document should not be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official. This document is not subject to copyright but attribution for its adoption and use would be appreciated by NIST.

Comments may be submitted to the Computer Security Division,
Information Technology Laboratory, NIST
via electronic mail at PIVaccreditation@nist.gov
or via regular mail at

100 Bureau Drive
Mail Stop 8930
Gaithersburg, MD 20899-8930

Acknowledgments

The authors wish to thank their colleagues who contributed to this document's development and reviewed its many versions. We would especially like to thank Ron Martin from the Department of Commerce; Kurt Kersch and Barry Colvin from the Department of Treasury, Internal Revenue Service; Miguel Calin from Mitre; Sarbari Gupta from Electrosoft; William MacGregor, Ketan Mehta, and Tanya Brewer from NIST for their technical inputs, Personal Identity Verification Card Issuer experience, SP 800-79-1 document preparation assistance and editorial suggestions. The authors also gratefully acknowledge and appreciate the many comments and contributions made by government organizations, private organizations, and individuals in providing direction and assistance in the development of this document.

TABLE OF CONTENTS

TABLES AND FIGURES

EXECUTIVE SUMMARY

Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, provided an impetus for major improvements in how personal identification credentials should be created, issued and used by the Federal government. The Directive requires development and use of standards for a secure and reliable form of identification for Federal employees and contractors. The standards and their specified Personal Identity Verification (PIV) system are to be used as a foundation for securely identifying every individual seeking access to valuable and sensitive Federal resources including buildings, information systems, and computer networks. Implementation and operation of the new PIV system will require the collection, access protection, and dissemination of large amounts of personal information, which itself requires privacy protection.

NIST developed and published Federal Information Processing Standard Document (FIPS) 201, entitled *Personal Identity Verification of Federal Employees and Contractors,* and several Special Publications providing additional specifications and supporting information in response to HSPD-12. These documents provide the required foundation for Government personal identification, verification, and access control systems.

In light of the requirements for both improved security and protection of personal privacy, HSPD-12 established four control objectives, one of which includes the call for a form of identification that is "issued by providers whose reliability has been established by an official accreditation process." In response, Appendix B of FIPS 201-1 specified that NIST "…establish a government-wide program to accredit official issuers of PIV Cards…," which led to development of this Special Publication. These Guidelines for the Accreditation of Personal Identity Verification Card Issuers will greatly assist in providing and assuring the reliability of issuers of the "secure and reliable forms of identification" required under HSPD-12.

The purpose of this Special Publication is to provide appropriate and useful guidelines for accrediting the reliability of issuers of personal identity verification cards and badges containing the identity credentials needed to verify the claimed identity of a person. The providers of secure and reliable identification perform the function of storing these credentials electronically on a smart card called the Personal Identity Verification (PIV) card, and issuing these cards to the authorized card holders. Hence these providers–the targets of assessment and accreditation as per the guidelines in this document–are called PCIs (PIV Card Issuers). Reliability of all issuers of PIV Cards is of utmost importance when one organization (e.g., Federal agency or Federal contractor) is required to trust the identity credentials of individuals issued by another organization. This trust will only exist if organizations have assurance that other organizations have developed and are using identity verification systems that are accredited as being operated with *consistent adherence to the standards developed in response to HSPD-12*. Adherence to all relevant policies, standards, and guidelines by a PIV Card Issuer on a continuing basis signifies and constitutes reliability.

With the goal of verifying that providers of secure and reliable identification credentials are consistently and reliably adhering to standards developed under HSPD-12, this Special Publication provides an assessment and accreditation methodology. This methodology includes

(i) specific requirements from FIPS 201-1 and supporting documents for PCIs; (ii) procedures for assessing and monitoring adherence to the requirements; and (iii) guidance for evaluating the results assessments prior to making an appropriate accreditation decision. If a PCI satisfies all the requirements from FIPS 201-1 and its supporting documents, as well as other relevant Federal policies and procedures through the specified assessment procedures, the PCI may be accredited– as required by HSPD-12–as being reliable.

Accreditation is one basis for trust for PCIs, and requires that all assessment and accreditation processes be thorough and comprehensive. Careful planning, preparation, and commitment of time, energy, and resources are required. These guidelines are designed to assist Agencies in creating the needed roles, assigning responsibilities, developing an acceptable operations plan, drawing a PCI's accreditation boundary, evaluating the findings of all reliability assessments, and making a proper decision for accrediting the PCI. Realizing that organizations may vary significantly in how they choose to structure their PCI operations, these guidelines have been developed to be flexible for supporting small organizations that are centrally located, large organizations that are geographically dispersed, and those organizations that out-source a majority of their operations to another organization. In addition to supporting organizational flexibility, these guidelines are designed to minimize the effort needed to assess, accredit, and monitor the continued reliability of a PCI.

In addition to flexibility and efficiency, the accreditation methodology which underlies these guidelines must generate assessment findings and resulting accreditation decisions that are consistent and repeatable. It is these latter characteristics that provide the assurance to an organization's management that when a PCI has been accredited based on these guidelines, the target of accreditation can be trusted as a provider of secure and reliable identification credentials as required by HSPD-12.

This document should be used by:

- Small organizations where all processes relating to PIV Card issuance are centrally located;
- Large organizations whose PIV Card issuance processes are geographically dispersed; and
- "Virtual" organizations that have out-sourced a majority of their processes to another organization or service providers.

1. INTRODUCTION

In order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy, the President issued Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractor*s, dated August 27, 2004. This Directive established a Federal policy to create and use a government-wide secure and reliable form of identification for Federal employees and contractors. It further defined *secure and reliable identification* as one that—

- Is issued based on sound criteria for verifying an individual employee's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

NIST developed and published Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and several Special Publications providing additional specifications and supporting information in response to HSPD-12. These documents provide the foundation for Government personal identification, verification, and access control systems.

Appendix B.1 of FIPS 201 states the following:

"… [HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. Funding permitting, NIST will establish detailed criteria that PIV Card issues must meet for accreditation. Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until such time as these are completed, agencies must self-certify their own issuers of PIV Cards. …"

In order to satisfy HSPD-12 and FIPS 201-1, NIST undertook the development of the Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations (hereafter called a PCI) and published them as NIST Special Publication (SP) 800-79. This document is the first revision of the original. The revised SP 800-79-1 provides a more technically based approach to assure that a PCI is fulfilling all the requirements of FIPS 201-1 and its supporting documents, and doing so reliably. In this revised document, a PCI is considered to be owned and managed by an *organization* which may be a Federal Department, Agency, private entity or other enterprise that desires to issue conformant and reliable PIV Cards. Ensuring the reliability of a PCI is of critical importance to the Federal government in light of the security and privacy implications of HSPD-12 and its far-reaching objective of issuing PIV Cards to millions of Federal employees and contractors. HSPD-12 and its implementing standards and guidelines were developed to address a range of security concerns including those posed by terrorists in a post-9/11 world. Providing a comprehensive set of standards for controlling access to the Federal government's physical and logical resources through the use of a standard PIV Card

assures that certain pre-defined levels of security can be achieved. However, it requires organizations to implement and use the standards in a consistent and reliable manner.

An organization must have confidence in the cards it issues to its own employees and contractors, but possibly more importantly since HSPD-12 requires a common inter-operable standard across the entire Federal government, all organizations need to have confidence in the cards issued by other organizations. This confidence can come about only if the PCI functions in those other organizations are assessed and accredited. Thus PCI accreditation forms an important task in meeting the end-goals of HSPD-12.

NIST has considerable experience in the development of accreditation methodology, most significantly with the widely accepted approach to accreditation in SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and its family of related documents. While SP 800-37 is focused on the accreditation of the security of information systems rather than the accreditation of the reliability of PCIs, it does offer a practical foundation for accreditation programs in general. This document utilizes various aspects of SP 800-37 and applies them to accrediting the reliability of PCIs. Accreditation of a PCI also requires accreditation of all information systems used by the PCI in accordance with SP 800-37.

One difference between accreditation of the security of information systems and the accreditation of the reliability of a PCI is that organizations have considerable flexibility in how they prepare for a SP 800-37 accreditation (particularly in implementing security controls), but have little room for variation under SP 800-79-1. Much of the flexibility in SP 800-37 comes from acceptable variations in security controls, a necessity since individual information systems in varied environments may have significantly different security requirements. Conversely, the desire for standardization implicit in HSPD-12 has led to the development of a rather stable set of requirements and specifications in FIPS 201-1. There may be some flexibility in how a requirement is achieved, but a majority of requirements must be satisfied in a uniform manner in order to obtain mutual trust among PIV adopting organizations. In many cases, a PCI has either satisfied a requirement by implementing and using a standard PIV component or service correctly and uniformly, or the PCI does not conform to the standard.

Although organizations may feel constrained by the uniformity required by FIPS 201-1, standardization greatly contributes to achieving the objectives of HSPD-12 across PIV Card Issuer implementations. For all organizations to accept the PIV Cards of other organizations, one set of rules (i.e., FIPS 201-1) must be followed by all PIV system participants. This Special Publication provides a way of determining if the participants are following these rules. Accreditation efforts that are consistent, reliable, and repeatable provide a basis for determining the *reliability* and capability of providers who issue PIV Cards, which herein is defined as *consistent adherence to the PIV standards.* In particular, if providers of PIV Cards meet the requirements of FIPS 201-1 and its supporting documents as verified through applicable assessment procedures and monitored over a period of time, they may be considered reliable as is required by HSPD-12.

The objectives of the guidelines in this document are to—

- Outline the requirements to be met by a PCI, the rationale for the requirements and the assessment procedures required to determine the satisfaction of those requirements by a PCI through a combination of policies, procedures, and operations.
- Describe an accreditation methodology that provides a framework for organizing the requirements and assessment procedures stated above and at the same time provides coverage for all the control objectives stated in HSPD-12.
- Demonstrate the fact that the application of the methodology will result in assessment outcomes that are consistent, reliable, and repeatable.
- Emphasize the role of risk in arriving at an accreditation decision based on assessment outcomes that takes into account the organization's mission.

1.1 Intended Audience

These guidelines are intended for organizations issuing or preparing to issue PIV Cards to employees, contractors, or other individuals conforming to FIPS 201-1 and complying with HSPD-12.

1.2 History of this Revision

In order to satisfy HSPD-12 and its tight time frame for compliance, SP 800-79 was developed shortly after publication of FIPS 201-1 in order to provide organizations an initial set of guidelines for the accreditation of their PIV Card Issuers. While the original version anticipated how PIV Card implementations and issuing organizations would develop, it was impossible to foresee how PCIs would actually evolve. Two years of PIV issuer accreditation experience has led to improved understanding of the diverse implementations of HSPD-12. Several changes and many improvements have been made to the original SP 800-79 based on feedback that NIST and the working group producing this revision have received.

The major changes for this revision include:

- Removal of attributes as the basis of assessments and replacing them with PCI controls traceable to specific requirements from FIPS 201-1 and related documents;
- Additional guidelines on how to determine the accreditation boundaries of a PCI;
- Discussion of the risk involved in authorizing the operation of a PCI;
- Removal of Sections 4.0 PCI Functions and Operations and 5.0 PIV Services and Operations which were narrative discussions of FIPS 201-1 requirements;
- Clarification of computer system security accreditation as specified in SP 800-37 and organizational reliability accreditation as specified in SP 800-79-1;
- Changing the term "certification" to "assessment"; and
- Use of "organization" instead of "department" or "agency."

1.3 Timelines for using the revised Guidelines

These revised guidelines for accrediting PCIs will take effect immediately following the final publication of SP 800-79-1. Hence, organizations should use these revised guidelines for accrediting any new PCI, any PCI whose accreditation is currently in progress, or any PCI that previously has gone through accreditation (under SP 800-79) and failed (with or without being issued a DATO or IATO). Any PCI that has already been accredited and currently holds the Authorization to Operate (ATO) under SP 800-79 must be re-accredited based on these revised guidelines no later than one year after the final publication date.

1.4 Key Related NIST Publications

The following NIST publications provide a standard and supporting specifications and guidelines to organizations implementing HSPD-12, and were utilized as the basis for requirements listed in this document.

- FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- Draft SP 800-73-2, *Interfaces for Personal Identity Verification*
- SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*
- SP 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
- SP 800-85B, *PIV Data Model Test Guidelines*
- SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*
- SP 800-104, *A Scheme for PIV Visual Card Topography*

1.5 Organization of this Special Publication

The remainder of this publication is organized as follows:

- **Chapter 2** provides background information needed to understand the PCI accreditation methodology as well as the inputs and outputs involved in the assessment and accreditation processes. These include: (i) Definition of the target accreditation entities (PCI, PCI facilities, PCI boundaries); (ii) the relationship between accreditation under SP 800-37 and accreditation under SP 800-79-1; (iii) preparatory tasks of accreditation including assignment of roles and responsibilities; (iv) three alternative accreditation decisions; (v) acceptance of risk in the accreditation decision; and (vi) the contents of the accreditation package.
- **Chapter 3** describes the building blocks of the PCI accreditation methodology including Accreditation Topics, Accreditation Focus Areas, and the control requirements within each area called PCI Controls.
- **Chapter 4** provides a detailed description of the assessment methods for the PCI controls whose outcomes form the basis for the accreditation decision.

- **Chapter 5** discusses assuring continued reliability of PCIs by extending the PCI accreditation methodology to include Accreditation Life Cycle Management (ACLM). The four phases of ACLM are described in this chapter.
- **Appendices** include— (i) references; (ii) glossary and acronyms; (iii) PCI Readiness Review Checklist; (iv) PCI operations plan template; (v) assessment report template; (vi) sample accreditation transmittal and decision letters; (vii) PCI controls and assessment procedures; and (viii) summary of tasks and sub-tasks.

2. THE FUNDAMENTALS

This chapter presents the fundamentals of PIV Card Issuer (PCI) accreditation including: (i) definitions of a PCI and a PCI Facility; (ii) outsourcing PCI services or functions; (iii) the differences between assessment and accreditation; (iv) the accreditation boundaries of a PCI; (v) roles and responsibilities; (vi) the relationship between accreditation under Special Publication (SP) 800-37 and SP 800-79-1; (vii) preparing for the assessment; (viii) the types of accreditation decisions; (ix) the use of risk in the accreditation decision; and (x) the contents of the accreditation package.

2.1 PCI

At the highest level, a PCI includes all the functions required to create, issue, and maintain Personal Identity Verification (PIV) cards for one or more organizations. A PCI is considered constituted if all relevant roles and responsibilities have been established; suitable policies and compliant procedures have been implemented within the areas of identity sponsorship, enrollment/identity proofing, adjudication, card production, card activation/issuance and maintenance; and the information system components utilized for performing the above-mentioned functions meet technical and operational requirements prescribed in FIPS 201-1 and its supporting documentation.

If an organization chooses to comply with Homeland Security Presidential Directive 12 (HSPD-12), it must first establish a PCI that conforms to, and satisfies the requirements of, FIPS 201-1 and its supporting documents. It must then be accredited under (i.e., using the guidelines specified in) SP 800-79-1. An organization has significant flexibility in establishing a PCI, and may choose to have multiple PCIs if there are significant variations in structural composition and mission within its operating units. Regardless of how a PCI(s) is structured, the organization (e.g., Federal agency, Federal contractor) is responsible for the management and oversight of the PCI and maintains full responsibility for the accreditation of the PCI as required in HSPD-12.

A PCI should be completely described in its operations plan. This comprehensive document pulls together all the information about the PCI so that any independent party that reviews it will be informed to the fullest extent of the PCI's operations. A PCI operations plan should include a wide variety of information, including a description of the structure of the PCI, its facilities, any external service providers, the roles and responsibilities within the PCI, policies and procedures which govern its operations, and a description of how requirements of FIPS 201-1 are being met. A template for a PCI operations plan is provided in Appendix D.

2.2 PCI Facilities

A PCI Facility (PCIF) is a physical site or location–including all equipment, staff, and documentation–that is responsible for carrying out one or more of the following PIV functions: (i) enrollment/identity proofing; (ii) card production; (iii) card activation/issuance; or (iv) maintenance. A PCIF operates under the auspices of a PCI, and implements the policies and executes procedures prescribed by the PCI for those functions for which the PCIF is authorized to operate (e.g. an enrollment/identity proofing facility, issuance facility).

Based on certain characteristics (e.g. size, geographic locations, organizations that it supports), a PCI may have its services and functions provided centrally or distributed across multiple locations. Independent of how or where a PCI implements these functions, at least one PCIF is required. For example, a geographically dispersed organization may decide to have enrollment/identity proofing and card activation/issuance functions performed in different facilities in different parts of the country so that PIV Card candidates can minimize travel. In this example, the different PCIFs fall under the purview (policy, management) of a single PCI which is defined to encompass all the functions necessary to issue PIV Cards. Within that PCI, the geographically dispersed PCIFs have specific responsibilities and are under the direct management control of the PCI.

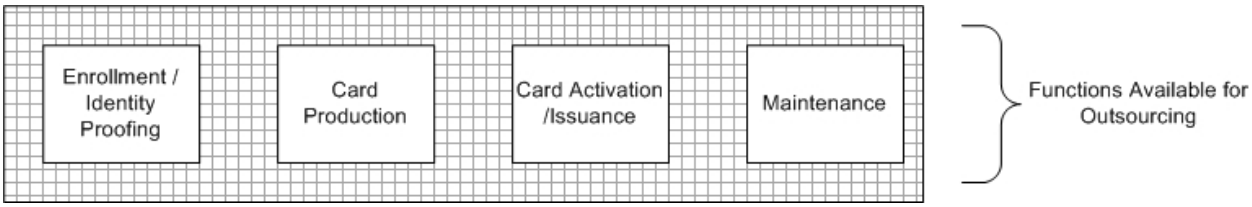

Figure 1 – Outsourcing of PCI Functions

2.3 Outsourcing of PCI Functions

Organizations may out-source one or more PCI functions to another organization. As the complexity and cost of new technology increase, organizations may decide that the most efficient and cost-effective solution for implementing HSPD-12 is to seek the services of an external service provider. An external service provider may be a Federal agency, a private entity, or some other organization that offers services or functions necessary to issue PIV Cards. Figure 1 provides an illustration of those areas that may be out-sourced. Not included in this list are two functions–sponsorship and adjudication. Only the organization which "owns" (i.e., manages, controls, or privately owns) the PCI can decide which of its employees, contractors, etc., should be submitted for consideration to receive a PIV Card (sponsorship) and under what standards the submission is approved (adjudication).

In addition to sponsorship and adjudication, a PCI which out-sources services to an external provider needs to assure that all privacy-related requirements are satisfied. The PCI is responsible for ensuring that privacy requirements are being met both for the internal information systems interacting with the external service provider's information systems as well as the personal information being handled within internal functions of sponsorship and adjudication.

If a PCI is using the services of an external service provider, they should review and approve the provider's operations plan and associated documents, the accreditation decision and evidence of implementations of FIPS 201-1 requirements. The resulting information must be included in the documentation that is reviewed during the PCI's assessments leading to accreditation.

2.4 Assessment and Accreditation

HSPD-12 has mandated that PIV Cards be "issued only by providers whose reliability has been established by an official accreditation process." This document contains guidelines for satisfying all the requirements for an official accreditation. It provides a methodology that any organization can utilize to formally accredit its PCI(s). This methodology consists of two major elements–assessment and accreditation. While assessment and accreditation are very closely related, they are two very distinct activities. Assessment, which occurs before accreditation, is the process of gathering evidence (generally by an independent party) regarding a PCI's satisfaction of the requirements of FIPS 201-1 and related documents, both at the organization and facility level. It typically includes interviews with PCI and PCIF personnel, a review of documentation, observation of processes, testing, and other activities needed to assess the PCI for conformance to FIPS 201-1 requirements. The result of these assessment activities is an assessment report that serves as the basis for an appropriate accreditation decision. The report is also the basis for a PCI corrective action plan (CAP) for removing or mitigating discovered deficiencies.

Distinct from assessment, accreditation is the decision of the Designated Accreditation Authority (DAA) to authorize operations of a PCI once they are confident that the requirements of FIPS 201-1 have been met and the risk regarding security and privacy is acceptable. The DAA must be knowledgeable of HSPD-12 as well as aware of the potential risks to its operations, assets, or individuals (e.g., PIV Card applicants, PCI Facility staff). In order that authorizing officials make informed, credible, and risk-based decisions regarding authorization, the assessment process should seek to answer the following questions:

- Has the PCI implemented the requirements of FIPS 201-1 in the manner specified therein?
- Do personnel understand the responsibilities of their roles and/or positions, and perform all required activities as described in the PCI's documentation?
- Are services and functions at the PCIF level (e.g., enrollment/identity proofing, card production, card activation/issuance, and maintenance) carried out in a consistent, reliable and repeatable manner?
- Have deficiencies identified during the assessment been documented, their current and potential impact on security and privacy highlighted, and the recommendations and timelines for their correction or mediation been included in the assessment report?

If these questions are answered during the assessment process, the organization's authorizing official will have sufficient information to make a correct decision concerning accrediting the PCI and authorizing its operation.

2.5 Accreditation Boundary for the PCI

An important initial task for the designated senior official within an organization preparing for an accreditation of their PCI is to identify the appropriate accreditation boundary. The accreditation boundary defines the specific PCI operations that are to be the target of the assessment and accreditation. A PCI comprises the complete set of functions required for the issuance and

maintenance of PIV Cards. In determining the accreditation boundary, the senior official may consider if the functions are being performed identically in all PCI facilities, are using identical information technology components, and are under the same direct management control. For instance, an organization may have two sub-organizations, each of which has distinct processes and management structures. The organization may decide to establish two separate PCIs, each with its own accreditation boundary. In this example, two separate assessments would be undertaken with each ending in an independent, but not necessarily different, accreditation decision.

In drawing an accreditation boundary, an organization may want to include only a subset of PCI Facilities. For example if a PCI has several facilities, some of which are ready for operation and some that are still in the development stage, the organization may choose to define the accreditation boundary to include the PCI and only those facilities that are ready to be assessed. If the accreditation is successful, the PCI and a subset of its facilities will be authorized to operate and begin issuing cards. The remaining PCIFs can continue with implementation and be assessed at a later date.

Within the mandate of HSPD-12, organizations have the freedom to determine how to provide secure and reliable identification. Some organizations may choose to offer PIV Card services entirely in-house, while other organizations may out-source functions such that the services being offered may not be under the direct management control of the organization nor physically located within its facilities. In the case of outsourcing, organizations must include the functions provided by external service providers within the accreditation boundary to make certain that they are included in the accreditation effort. This assures that irrespective of how and where the functions are performed, the organization maintains complete accountability for the reliability of its PIV program.

Careful consideration should be put into defining the accreditation boundary for a PCI. A boundary that is unnecessarily expansive (i.e., including too many dissimilar processes and business functions, geographically dispersed facilities, etc.) makes the assessment and accreditation process extremely unwieldy and complex. On the other hand, a boundary that is unnecessarily limited increases the number of needed assessments and accreditations and thus drives up the total cost for an organization. An organization should strive to define the accreditation boundary for a PCI that strikes a balance between the costs and benefits of assessment and accreditation.

While the above considerations should be useful to an organization in determining the boundary for its PCI for purposes of accreditation, they should not limit the organization's flexibility in establishing a practical boundary that promotes an effective HSPD-12 compliant implementation. Authorizing officials and other senior organization officers should consult with PCI facility managers and other potentially affected organizational personnel when establishing a PCI's accreditation boundary. Establishing a boundary for a PCI and its subsequent accreditation are organization-level activities that should include participation of all key personnel. Establishing the boundary should take into account the goals of HSPD-12 and the risks to the organization and others that rely on this secure, reliable, and inter-operable PCI. The costs of accrediting and operating the PCI should also be taken into account when establishing the boundary.

2.6 PCI Roles and Responsibilities

This section describes the roles and responsibilities of key personnel involved in the accreditation of a PCI. Recognizing that organizations have widely varying missions and structures, there may be some differences in naming conventions for accreditation-related roles and in how the associated responsibilities are allocated among these personnel (e.g. one individual may perform multiple roles).

2.6.1 Senior Authorizing Official

The Senior Authorizing Official (SAO) (see Figure 2) of an organization is responsible for deployment of all PCI operations. An SAO should have budgetary control, provide oversight, develop policy, and have the final review authority over accrediting and approving operation of the PCI.

2.6.2 Designated Accreditation Authority

The Designated Accreditation Authority (DAA) is an official of the organization with the authority to review all assessments of a PCI and its facilities, and to accredit the PCI as required by HSPD-12. Through accreditation, the DAA must accept responsibility for the operation of the PCI at an acceptable level of risk to the organization. In some organizations, the SAO could perform the role of the DAA.

2.6.3 Organization Identity Management Official

The Organization Identity Management Official (OIMO) is responsible for implementing policies of the organization, assuring that all specified procedures of the PCI are being performed reliably, and providing guidance and assistance to the PCI. The OIMO implements and manages the PCI's operations plan; ensures that all PCI roles are filled with capable, trustworthy, knowledgeable, and trained staff; makes certain that all PCI services, equipment, and processes meet FIPS 201-1 requirements; monitors and coordinates activities with PCI Facility Manager(s); and supports the accreditation process.

2.6.4 PCI Facility Manager

A PCI Facility Manager manages the day-to-day operations of a PCI facility. A PCIF Manager is responsible for implementing standard operating procedures for those functions that have been designated for that facility. The Manager must ensure that all PIV processes adhere to the requirements of FIPS 201-1, and that all PIV services performed at the PCIF are carried out in a consistent and reliable manner in accordance with the OIMO's direction.

2.6.5 Assessor

The Assessor is an individual, group, or organization that is responsible for performing a comprehensive and independent assessment of a PCI. The Assessor gathers evidence as to whether there are discrepancies between the current status of the PCI and its facilities and the requirements of FIPS 201-1. These assessment findings are presented to the organization's DAA who uses them as the basis for the decision to authorize the PCI operations. The Assessor should also provide recommendations to the DAA for reducing or eliminating deficiencies and security weaknesses, describing the potential impact of those deficiencies if not corrected.

2.6.6 Privacy Official

The responsibilities of the Privacy Official (PO) are defined in FIPS 201-1. The person filling this role shall not assume any other operational role in the PCI. The PO issues policy guidelines with respect to collection and handling of credentials and other personally identifiable information from PIV Card applicants so as to ensure that the PCI is in compliance with all relevant directives of the privacy laws. The PO's role may be filled by an organization's existing official for privacy (e.g., a Chief Privacy Officer).

2.6.7 Delegation of Roles

Although PCI roles are independent and should be filled by different people if feasible, there may be a need (availability, economy) to have one person fill more than one role. Except for the roles of Assessor and Privacy Official, one person may perform more than one role if needed. There also may be occasions when an organization has multiple PCIs. In this case, one person may be assigned the same role in several PCIs. For instance, a SAO may provide oversight to several PCIs within the organization. Of the roles described, the SAO, DAA, PO and OIMO must be Federal employees.

2.6.8 Roles in PCI Facilities

Figure 2 below illustrates a possible role structure when a PCI has multiple PCIFs. The SAO has the primary authority and responsibility for the PCI. Reporting to the SAO are the OIMO and the DAA. A PCI Facility Manager is responsible for managing operations at each PCI facility and reports to the OIMO. The dotted lines leading to the PO and the Assessor indicate their independence from the day to day operations of the PCI.

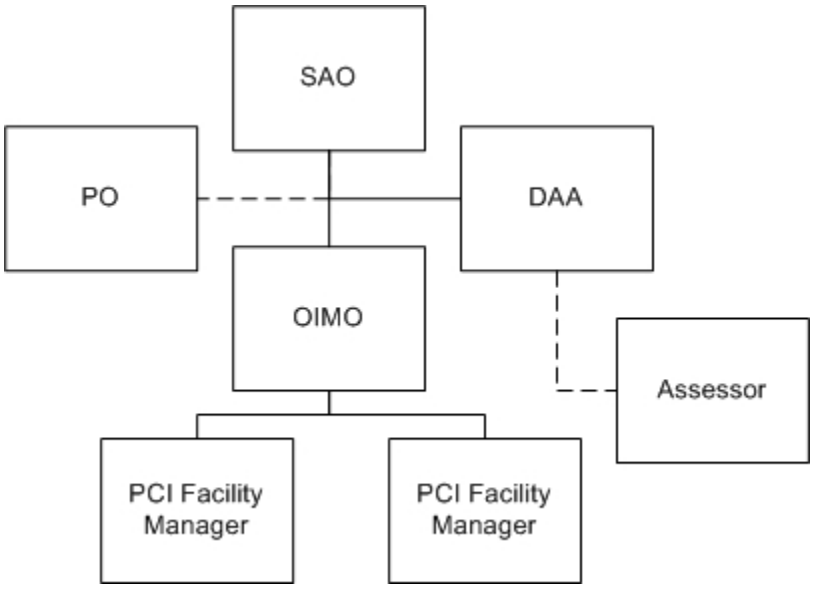

Figure 2 - PCI Roles

2.7 The Relationship between SP 800-79-1 and SP 800-37

While accreditation is the major topic of both special publications, the goals of accreditation are distinct in SP 800-37 and SP 800-79-1. Accreditation under SP 800-37, as mandated by Appendix III of the Office of Management and Budget (OMB) Circular A-130, focuses on "authorizing processing" of information systems based on an assessment of security at the information system level. Accreditation as discussed herein and as mandated by HSPD-12 is concerned with the assessment of the "reliability" of a PCI to perform its functions in accordance with FIPS 201-1. An accreditation decision granted under SP 800-37 signifies that an organization official accepts responsibility for the security (in terms of confidentiality, integrity, and availability of information) of the information system. Accreditation of a PCI's reliability under SP 800-79-1 indicates that the organization official agrees to accept the risk that the PCI can operate within the control objectives outlined in HSPD-12 for "secure and reliable forms of identification." However, in both cases, the organization official accepts responsibility for the PCI and the PIV Cards that it issues, and is fully accountable for any adverse impacts to the organization if a breach in security, privacy, or policy occurs.

SP 800-79-1 focuses on accreditation of capability and reliability at an organizational level, but depends on adequate security for all the supporting information systems that have been accredited under SP 800-37. Therefore, before the organization official accredits the PCI and its facilities, the PCI information system(s) used must be accredited.

In many cases, accreditation under SP 800-37 will be granted by an organization official different than the official responsible for accrediting the PCI. The former is an organization official tasked with making a decision on whether to authorize operation of an information system based on its security posture. The latter must be someone designated specifically for authorizing the operation of the PCI after it has been accredited.

2.8 Preparing for a PCI's Assessment

To facilitate an assessment of a PCI in a timely, efficient, and thorough manner, it is essential that all members of the Assessment team and staff of the PCI understand their specific roles and responsibilities and participate as needed. The PCI, its facility personnel, and the team responsible for performing the assessment must cooperate and collaborate in a joint manner to ensure the success of the assessment. Specific responsibilities of the assessment team are listed below. For further information, including considerations organizations may want to take into account when outsourcing assessments, refer to NIST Interagency Report (IR) 7328 *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems*

2.8.1 PCI Duties

Before the assessment can begin, the DAA must choose an Assessor (usually an assessment team and leader) and identify needed PCI assessment services. These may be provided within the organization or may be a public or private sector entity contracted to provide services. Members of the assessment team should demonstrate a variety of different capabilities required to perform the necessary activities specified in this document. The assessment provider should have an appropriate management structure to oversee the personnel conducting the assessment. The

assessment provider should be able to perform administrative functions to support the assessment team, protect the information received from the customer, and develop and implement standard procedures to ensure that all assessment teams provide consistent and reliable assessment services.

Assessment team members should work together to prepare for, conduct, and document the findings of the PCI's assessment and assessments of all PCI facilities within the PCI boundary. Each team must be made up of individuals that collectively have the knowledge, skills, and abilities to conduct, evaluate, and document all assessments including those performed on the information systems within the PCI.

Once an assessment provider is chosen, the OIMO and other relevant PCI personnel should begin the preparation for the assessment. Thorough preparations by both the PCI and the assessment team are important aspects of conducting an effective assessment. The PCI sets the stage for the assessment by identifying all appropriate personnel and making them available during the assessment. A fundamental requirement for accreditation is interviews by the assessment team of all PCI personnel. Personnel and officials must be notified of the pending assessment, must understand their role in the process, and must be made available in accordance with the planned assessment schedule.

The OIMO must ensure that all relevant documentation has been completed and organized before the assessment begins. This documentation is comprised of policies and procedures, organizational structure, information system architecture, product and vendor details, and specifics regarding the implementation of all the requirements from FIPS 201-1 and related publications. If the PCI has out-sourced functions to an external service provider, they must obtain all necessary documentation from the provider regarding those operations utilized by the PCI. Before providing any documentation to the assessment team, the OIMO must review it to make certain it is both current and approved.

Another significant activity during the assessment is the observation by the assessment team of actual processes followed by the PCI. In order for the assessment team to confirm that processes are implemented in accordance with the operations plan, the PCI will need to ensure that assessment team members have access to PCI processes in real time. This could include scheduling enrollment/identity proofing, adjudication, card production, card activation/issuance, and maintenance activities for observation by the assessment team.

In order to aid the PCI's planning and preparation for the assessment, Appendix C includes a readiness review checklist. The checklist contains items needed during the assessment process. Satisfying this list of items before the assessment commences will facilitate the assessment and save significant time and energy during the process.

2.8.2 Assessment Team Duties

The independence of the assessment team is an important factor in assessing the credibility of the assessment results. In order to guarantee that the results of the assessment are impartial and unbiased, an effort must be made to ensure that members of the assessment team are not involved in the development, day-to-day maintenance and operations of the PCI, or in the removal, correction, or remediation of deficiencies.

The assessment team may obtain information during an assessment that the organization does not want to disclose publicly. The assessment team has an obligation to safely and securely store and protect the confidentiality of all security assessment related records and information, including limiting access within their organization to the individuals that need to know the information. When using, storing, and transmitting information related to the PCI assessment, the assessment team shall follow guidelines established by the organization in addition to other relevant laws, regulations, and standards regarding the need, protection, and privacy of information.

2.9 Accreditation Decisions

An accreditation decision is a judgment made by the DAA regarding authorizing operation of a PCI and its facilities. The DAA reviews the results of the assessment, considers the impact to the organization of any identified deficiencies, and then decides whether to authorize the operation of the PCI and its facilities. In doing so, the DAA is agreeing to accept the security and privacy risks to the organization in issuing and maintaining PIV Cards.

During the accreditation decision process, the DAA must evaluate the assessment findings for the PCI and each facility as defined in the accreditation boundary. If the PCI has out-sourced some of its services or functions, the DAA must review any accreditations that have been granted to the external service provider and include them as a part of the overall evaluation of risk to the organization.

An authorization decision by a DAA is always granted for a specific PCI, and for every PCI there can be only one authorization decision. In issuing this decision, the DAA must indicate the PCI accreditation boundary to which the authorization applies. A DAA grants an authorization to a PCI and then specifies which facilities are permitted to operate under that authorization. This allows the PCI and any authorized facilities to begin operations while any remaining facilities focus on addressing deficiencies with FIPS 201-1 and its supporting documents. At a later date, these facilities can be reassessed. The DAA, after reviewing the new findings, can reissue the authorization for the PCI and expand the accreditation boundary to which the authorization applies by including the newly assessed facilities.

The major input into the accreditation decision is the assessment report. To ensure the assessment report is properly interpreted and the reason for the accreditation decision properly communicated, the DAA should meet with the Assessor, the OIMO, and the PCI Facility Manager(s) prior to issuing an accreditation decision to discuss the assessment findings and the terms and conditions of the authorization. There are three accreditation alternatives that can be rendered by the DAA:

- Authorization to operate;
- Interim authorization to operate; or
- Denial of authorization to operate.

2.9.1 Authorization to Operate

If, after reviewing the results of the assessment phase, the DAA deems that the PCI and its facilities conform to FIPS 201-1 and its supporting documents to an acceptable degree, and will continue to do so reliably during the accreditation period, an *authorization to operate* (ATO)

may be issued. The PCI and its facilities are authorized to perform without restrictions or limitations those services that can be performed in compliance with all relevant policies, in conformance to all relevant standards, and in accordance with the documented operations plan. An ATO may be granted to a PCI and all of its acceptable PCIFs even if one PCIF has deficiencies. However, that PCIF cannot be authorized to operate. The DAA shall indicate in the ATO exactly which facilities are included as being authorized to operate along with any limitations imposed.

After receiving an ATO under SP 800-79-1, re-accreditation shall be performed within three years or when there is a significant change within the operations of a PCI. For instance, if additional facilities are to be included under the ATO, a re-accreditation should be undertaken.

2.9.2 Interim Authorization to Operate

If, after reviewing the results of the assessment phase, the DAA deems the discrepancies to be significant but there is an overarching necessity to allow the PCI and its facilities to operate, an *interim authorization to operate (IATO)* may be issued. An interim authorization to operate is rendered when the identified deficiencies in the PCI and its facilities are significant but can be addressed in a timely manner. These deficiencies must be documented within the Corrective Action Plan. An interim authorization is an authorization to operate under specific terms and conditions. The DAA shall indicate in the IATO exactly which facilities are included as being authorized to operate during this interim period along with any limitations imposed. It is recommended that the maximum duration of an IATO be three months. A maximum of two (2) consecutive IATOs may be granted for a PCI. Failure to correct deficiencies found in the PCI after the expiration of the second IATO must result in an issuance of a denial of authorization to operate (DATO) for the PCI.

A PCI is *not considered* accredited during the period of an IATO. When the deficiencies have been corrected, the IATO should be replaced with an ATO. Significant changes in the status of the PCI that occur during the IATO period shall be reported immediately to the DAA.

2.9.3 Denial of Authorization to Operate

If, after reviewing the results of the assessment phase, the DAA deems operation of the PCI to be unacceptable, a *denial of authorization to operate (DATO*) is transmitted to the OIMO. Failure to receive authorization to operate indicates that there are major deficiencies in reliably meeting the requirements of FIPS 201-1. The PCI is not accredited and must not be allowed to operate. If the PCI is currently in operation, all functions must be halted including operations in its facilities. If the PCI was previously accredited and had issued PIV Cards under an ATO, the OIMO along with the PCIF Manager(s) should consider whether a revocation of PIV Cards is necessary. The DAA and the Assessor should work with the OIMO and PCIF Manager(s) to ensure that proactive measures are taken to correct the deficiencies.

A PCI must not be authorized to operate if one or more of its critical information system(s) has not been accredited or is issued a DATO under SP 800-37. In the case where an IATO (under SP 800-37) has been issued for an information system within the PCI, the DAA should only issue an IATO to the PCI. Once the SP 800-37 IATO is replaced with an SP 800-37 ATO, the DAA can issue a SP 800-79-1 ATO. If during the course of operation of a PCI the SP 800-37 ATO expires

for one or more of information systems, the OIMO shall assess the criticality of the system for PCI operations and present the analysis to the DAA. The DAA then can exercise the following options:

- Set a timeline for the systems under PCI to be re-accredited under SP 800-37 without making any change to PCI's ATO status;
- Downgrade the current SP 800-79-1 ATO to an IATO; or
- If circumstances warrant, issue a SP 800-79-1 DATO and halt all PCI operations.

2.10 The Use of Risk in the Accreditation Decision

Accreditation is the official management decision by the DAA to authorize operation of a PCI based on an assessment of its reliability and an acceptance of the risk inherent in that decision. By granting an authorization to operate, the DAA accepts responsibility for the reliability of the PCI and is fully accountable for any adverse impact to the organization or any other organization from cards issued by the PCI, its facilities, and any external service providers.

The assessment of a PCI provides the DAA with the basis not only for determining its reliability, but also determining whether to accept the risk to the organization in granting an ATO. As the requirements in FIPS 201-1 and related documents form the basis of the assessment and are ultimately derived from the control objectives of HSPD-12, those not reliably met by the PCI and its facilities represent the potential for adverse impact.

Implementation of an HSPD-12 program exposes an organization to specific risks at the mission level of the organization. The PIV Card is used to establish assurance of the identity of the cardholder, and as such, it must be trusted as a means for which access to logical and physical resources can be granted. Any problem with an issued PIV Card that undermines that assurance could expose an organization to harm. Furthermore, the collection, processing and dissemination of significant amounts of personal information required to issue a PIV Card increases the threat of this information being used for malicious purposes. It is the DAA's responsibility to weigh the risks of these and other security and privacy impacts of issuing PIV Cards when making the accreditation decision.

Furthermore, as HSPD-12 is a government-wide mandate based on a standard of interoperability allowing organizations to accept other organizations' PIV Cards, accreditation decisions within a single organization directly impact other organizations. An inter-operable credential creates an opportunity for the provisioning of access to physical and logical resources between organizations. The DAA's signature on the accreditation letter signifies their acceptance of responsibility (i.e., accountability) for the operations of the PCI not only to the issuing organization but to other organizations that are linked together in a federated circle of trust that can only be as strong as its weakest link.

2.11 Accreditation Package and Supporting Documentation

The *accreditation package* documents the results of the assessment phase and provides the DAA with the essential information needed to make a credible, risk-based decision on whether to

authorize operation of the PCI. Unless specifically designated otherwise by the DAA, the OIMO is responsible for the assembly, compilation, and submission of the accreditation package. The accreditation package contains the following documents:

- The PCI's operations plan (including any PCI Facilities Standard Operating Procedures [SOPs] and attachments)
- SP 800-37 accreditation letters
- The assessment report
- The corrective action plan

The PCI's operations plan is prepared by the OIMO and approved by the SAO. It is the central location where the PCI's policies, procedures, and processes for all the major functional areas are documented. In this regard, the operations plan provides a complete picture of the structure, management, and operations of the PCI to the Assessor and DAA. Appendix D provides a template of what to include in the PCI operations plan. Perhaps most significant in the operations plan is the list of PCI controls, how they were implemented, and who is responsible for their management. This description of the PCI controls makes it a simple process for the Assessor to quickly ascertain how they were implemented and by whom.

If certain functions described in the operations plan are out-sourced, the PCI's operation can reference or "point to" the external service provider's operation plan and related documentation such as support agreements and any contracts. In this manner, the assessor has access to the information regarding the external service provider's operations without requiring the PCI to duplicate any documentation.

The SP 800-37 accreditation letters are the formal authorization to operate the PCI information systems. During the accreditation of the PCI under this Special Publication, the DAA should review any SP 800-37 accreditation letters for information systems which are directly involved in the issuance and maintenance of PIV Cards.

The PCI assessment report, prepared by the Assessor, provides the information needed to determine the extent to which the requirements are being met and are expected to continue as such during future operations. For each deficiency that is found, the assessment report must include the potential impact of the deficiency if it continues without correction and the recommended corrective action to correct it. Appendix E provides a template of what to include in the assessment report.

The corrective action plan (CAP), prepared by the OIMO with the assistance of the Assessor, describes the changes needed: (i) to correct deficiencies noted during the assessment with a time frame for completion; and (ii) to reduce or eliminate vulnerabilities in creating and issuing secure and reliable PIV Cards.

The OIMO submits the accreditation package to the DAA.[1] Figure 3 illustrates the primary sections of the accreditation package.

[1] Accreditation packages may be submitted in either paper or electronic format. Appropriate measures should be employed to protect the information contained in accreditation packages (electronic or paper format) in accordance with organization policy.

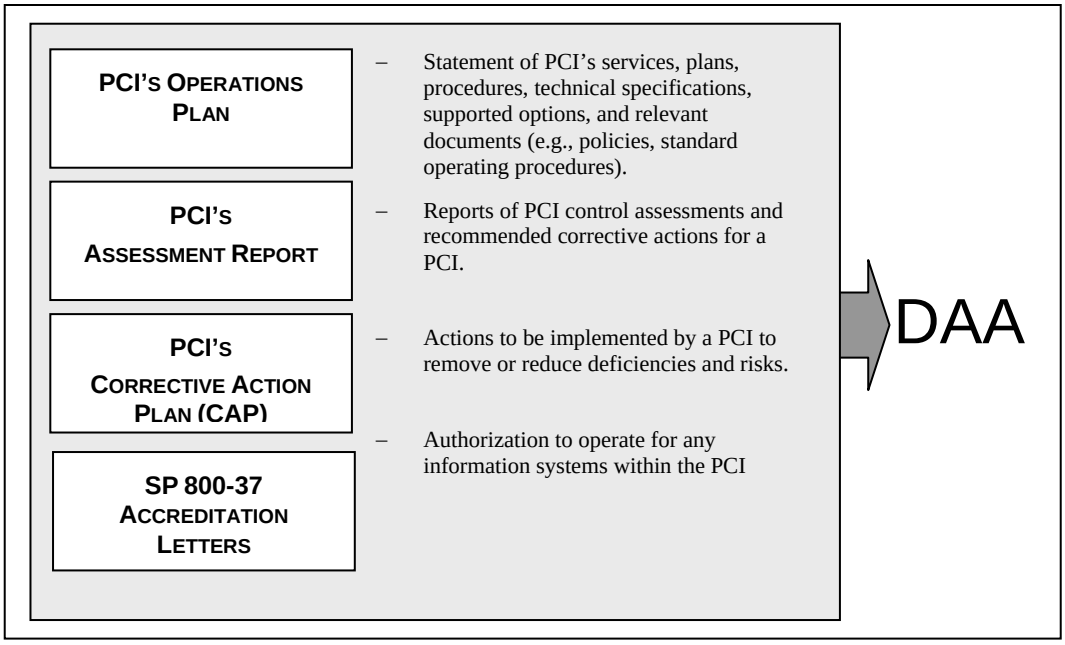

Figure 3 - Accreditation Package

Upon receiving and reviewing the accreditation package and in consultation with the Assessor, the DAA decides whether to authorize operations of the PCI. The accreditation decision letter transmits the accreditation decision from the DAA to the OIMO. The accreditation decision letter contains the following information:

- Accreditation decision;
- Supporting rationale for the decision; and
- Terms and conditions for the authorization including which PCIFs are included within the decision.

The accreditation decision letter (see Appendix F for examples) informs the OIMO that the PCI is: (i) authorized to operate; (ii) authorized to operate on an interim basis; or (iii) not authorized to operate. The supporting rationale includes the justification for the DAA's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the PCI including which PCIFs are to be included in the decision. The accreditation decision letter is attached to the original accreditation package and maintained along with the other PCI documentation.

Upon receipt of the accreditation decision letter and accreditation package, the OIMO reviews the terms and conditions of the authorization. The DAA also retains a copy of the accreditation decision letter and accreditation package. The accreditation-related documentation (especially information dealing with vulnerabilities) is: (i) marked and protected appropriately in accordance with organization policy; and (ii) retained in accordance with the organization's record retention policy.

3. PIV CARD ISSUER (PCI) COMPLIANCE

3.1 Introducing PCI Controls

Accreditation of a PCI is a broader endeavor than an accreditation of the security of an information system under SP 800-37. The requirements for a PCI as specified in FIPS 201-1 and related documents cover all major aspects of a PCI including infrastructure, organizational preparedness, security management, and data protection measures and processes. Each broad area is defined herein as a PCI Accreditation Topic (PAT). In addition to providing structure to the assessment, PATs are also used to summarize the assessment results for reporting. They also are used to structure the report to senior organization officials analyzing the areas of strength and weakness within the PCI.

The four PCI Accreditation Topics are:

Organizational Preparedness relates to the overall level of engagement of senior management regarding the formation and operation of the PCI. Roles and responsibilities must be clearly identified, and policies and procedures must be defined, documented, and put in place.

Security Management & Data Protection concerns the provisioning of adequate measures (e.g., management procedures, technical protections) to ensure that privacy requirements are addressed, the rights of individuals are acknowledged, and personal data are protected.

Infrastructure Elements represents the sum of the activities required to procure, deploy, and maintain the PCI information system components. PCI information system components (PKI, biometrics, card production, etc.) must meet the technical specifications defined in Federal Information Processing Standard (FIPS) 201-1 and related documents. Additionally, information systems used within the PCI need to be certified and accredited under Special Publication (SP) 800-37.

Processes involves the major functions involving managing a PIV Card throughout its life-cycle, including sponsorship, enrollment/identity proofing, adjudication, card production, card activation/issuance, and maintenance.

Each PAT is sub-divided into one or more Accreditation Focus Areas. Each focus area is a set of requirements that need to be met by the PCI and its facilities. Each requirement and the procedure, process, or technical product (termed a “PCI control”) used to satisfy each requirement listed under a focus area needs to be satisfied by a PCI. However, the manner in which the requirement is satisfied, and its specifications are implemented and managed, may vary from organization to organization.

For instance, each PCI is required to identity proof their applicants prior to enrollment. This process can be implemented in one of several ways depending upon the structure, size, and geographical distribution of an organization’s facilities. The process could be conducted at a central location or could be distributed throughout the country within regional centers. It could

be operated directly by the organization or by an outside service provider. However, irrespective of the implementation approach, this enrollment/identity proofing activity needs to be performed.

PCI controls are designed to satisfy specific requirements of FIPS 201-1 and related documents, and their implementation is mandatory. PCI controls ensure conformance with FIPS 201-1 as mandated by HSPD-12. Failure to implement any one of the PCI controls may directly impact the capability and reliability of the PCI and its facilities in issuing and maintaining PIV Cards, and thus increase levels of risk to the organization and its mission. The exception to this rule is when a suggested specification is optional or may be satisfied in alternative ways. For example, it is not mandatory that an organization stores an electronic image of the cardholder in the memory of a PIV Card. However, if they choose to do so, it must follow the formatting specifications provided in SP 800-76-1.

The evidence that ensures the presence of PCI Controls that are derived from FIPS 201 and related document requirements, and revealed through appropriate assessments, establishes the capability of a PCI. However, accreditation is generally based not merely on the demonstration of capability but also on the presence of certain organizational characteristics that will provide a high degree of confidence to the assessor that the demonstrated capabilities will be carried out in a dependable and sustainable manner. This dependability measure, or reliability (as it is generally called), has to be established by adequately assessing that a PCI has the desired organizational characteristics, including appropriate facilities, equipment, trained personnel, adequate resources, trustworthy management, and properly vetted operations staff.

Hence our accreditation methodology includes certain PCI establishment-level controls under the accreditation focus area entitled “Facility and Personnel Readiness”. These PCI establishment-level controls are formulated based on “commonly accepted security readiness measures” that have evolved in response to lessons learned in security incidents that have taken place due to threats, such as insider attacks, and risks, such as physical security lapses.

The four PIV Accreditation Topics discussed above and the Accreditation Focus Areas under each of these topics are listed in Table 1 below:

Organizational Preparedness
Preparation and Maintenance of Documentation (DO)
Assignment of Roles and Responsibilities (RR)
Facility and Personnel Readiness (FP)
Security Management & Data Protection
Protection of Stored and Transmitted Data (SY)
Enforcement of Applicable Privacy Requirements (PR)
Infrastructure Elements
Deployed Products & Information Systems (DP)
Implementation of Credential Infrastructures (CI)
Processes

Sponsorship Process (SN)
Enrollment/Identity Proofing Process (EI)
Adjudication Process (AD)
Card Production Process (CP)
Card Activation/Issuance Process (AI)
Maintenance Process (MP)

Table 1 - PATs and Associated Accreditation Focus Areas

Appendix G contains required PCI controls grouped by PAT and Accreditation Focus Area. Each PCI control represents how one or more requirements from FIPS 201-1 can be satisfied. PCI controls are sequentially numbered using the two-character identifier assigned to the Accreditation Focus Area under which they are listed. Included with each PCI control are acceptable assessment procedures. Table 2 shows the relationships between PATs, Accreditation Focus Areas, and PCI controls.

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Preparation and Maintenance of Documentation (DO)	DO-1	The organization develops and implements an operations plan according to the template in Appendix D. The operations plan references other documents as needed.	SP 800-79-1, Section 2.11 – Accreditation Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for enrollment/identity proofing which are approved by the DAO.	FIPS 201-1 2.2 PIV Identity Proofing and Registration Requirements

Table 2 - PAT, Accreditation Focus Area, and PCI Control Relationships

Irrespective of whether the information systems utilized within the PCI and its facilities are categorized at low, moderate, or high impact levels according to FIPS 199, the same set of PCI controls apply regardless of an individual system's impact level. More specifically, SP 800-53A provides a listing of standard information-system security controls that need to be implemented by an information technology asset based on the information-system security categorization level. On the other hand, the PCI control set represents a standard baseline of controls that must be implemented by the PCI and its facilities to be compliant with the requirements of FIPS 201-1. However, there is nothing precluding a PCI from implementing additional PCI Controls to ensure a higher level of confidence in mitigating risks associated with issuing PIV Cards.

3.2 Implementing PCI Controls

Each PCI Control must be properly implemented, managed, and monitored in order conform to FIPS 201-1. Depending on how an organization decides to implement its HSPD-12 program, these controls may not be under the direct management of the OIMO. However, the SAO is still responsible for ensuring the PCI controls are implemented correctly, operating as intended, and producing all desired results.

3.2.1 PCI Controls implemented at the Organization or Facility Level

Organizational PCI controls are implemented and managed at the organization level, and must not be impacted by operations at the facility level. For instance, the PCI control requiring quarterly reporting to OMB of the number of PIV Cards issued must be met by the PCI as a whole, and must be independent of any operations performed at the facility level.

A facility-specific PCI control covers specific functions managed and performed by the PCI Facility (e.g., fingerprinting the applicant prior to enrollment/identity proofing). Each PCI Facility within the PCI with enrollment/identity proofing responsibilities must assure use of this PCI control independently of the others.

If a PCI decides to out-source a function (e.g. card production), it will be dependent on an external service provider to implement the needed PCI controls. Even though the function was out-sourced, the PCI is still responsible and accountable for ensuring that the service provider uses, enforces, and maintains all applicable PCI control(s).

A PCI control may be implemented at both the organization level and the facility level. This determination must be made by each organization based on their HSPD-12 compliance policy and regulations. The description of the PCI control states if it needs to be implemented by the organization or at each facility.

4. ASSESSMENTS

An assessment is a set of activities performed by the Assessor to gain assurance that the PIV Card Issuer (PCI) controls have been implemented properly and meet their required function or purpose. Understanding the overall effectiveness of the PCI controls implemented in the PCI and its facilities is essential in determining the risk to the organization's overall mission and forms the basis for the accreditation decision by the Designated Accreditation Authority (DAA).

An Assessor must: (i) compile evidence that PCI controls employed in the PCI are implemented correctly, operating as intended, and producing the desired results; and (ii) present this evidence in a manner so that the DAA is able to effectively make a credible, risk-based decision about the operation of the PCI.

The basis for the assessment is the PCI controls, each of which is designed to represent specific requirements from Federal Information Processing Standard (FIPS) 201-1 and related documents. The objective for the Assessor is to use the assessment procedures associated with each PCI control (described in Appendix G) as a means to measure if the PCI being assessed meets the requirements described by FIPS 201-1. The assessment procedures are designed to facilitate the gathering of evidence that PCI controls are implemented correctly, operating as intended, and producing the desired outcome.

In preparation for a PCI assessment, the Assessor must first review the accreditation boundary to understand the target of the assessment. The accreditation boundary informs the Assessor as to which PCIFs and out-sourced service providers are to be included in the assessment.

The second step for the Assessor is to review the PCI operations plan to determine which PCI controls are implemented at the organizational level and which are implemented at the facility level. This analysis is critical as it provides the Assessor with an understanding of where different areas of responsibility lie within the PCI and how to address them during the assessment.

In cases where a PCI has out-sourced functions, the PCI will be responsible for ensuring that the external service provider has implemented the control. During the assessment, it is the service provider's responsibility to provide documentation to the Assessor regarding the implementation of that control. If results from a previous assessment of the service provider can be referenced, the Assessor may elect to incorporate these results or redo part or all of the assessment.

For those PCIs that include more than one facility, PCI controls that are designated as organizational can be assessed once and applied to the entire PCI after assuring that they are performed as required within in PCI Facility (PCIF). Additional assessments will be needed when additional PCIFs are added to the PCI, but these organizational controls need only be reassessed and reaffirmed at the PCI level. However, it is up to the discretion of the DAA whether a previously assessed PCI needs to be reassessed.

Facility-specific PCI controls must be assessed individually at each facility where they are deployed. For a PCI with multiple facilities utilizing identical procedures and processes, the DAA may elect to assess a randomly selected PCIF and use a method of sampling to assess PCI control implementations at the other facilities.

Past assessments may be used as a starting point for the assessment of a PCI. While past assessments will provide insight into the implementation and operation of the PCI, a number of factors affect the validity of past assessments. These include the passage of time, updates in policies and procedures, changes in technology, and turnover in employees and contractors. Assessors must validate whether a PCI is currently operating as expected using the given assessment procedures, as well as specially tailored or augmented procedures which may be desired. It is only through current validation and assessment of PCI controls that the Assessor and OIMO will have confidence in the reliability of the PCI and its facilities.

Use of automated security controls in information systems results in greater assurance of the protection of information and other organizational assets if reliably implemented and maintained. Human involvement results in significantly more variability in how PCI controls are implemented and operated, as security and reliability depend on an individual's training, knowledge, motivation, experience, and management along with other factors. Reliance on humans for data protection rather than reliable, automated security mechanisms makes it critical that trust and reliability assessments of management, operations, and maintenance personnel are current and up-to-date. Many of the assessment procedures rely on sensitive interactions among Assessor, PCI management, and facilities staff. Included are interviews with all involved personnel and observations of all PCI processes in real-time operation. In essence, on-site visits, real-time observations, and reviews of processes are essential as the Assessor must not rely solely on documentation to determine whether a given policy or procedure has been implemented and is being reliably utilized.

4.1 Assessment Methods

Associated with each PCI control listed in Appendix G, there are one or more assessment procedures. An assessment procedure consists of all the activities to be performed by the Assessor. For each control, one or more of the following assessment methods are listed:

- *Review* – an evaluation of documentation (plans, policies, procedures) with the goal of evaluating them as being adequate, understood by the PCI management and operations personnel, and being used in accordance with applicable policies, regulations, standards, technical guidelines, and organizational guidance.
- *Interview* – a directed conversation of an assessor with one or more PCI personnel in which both pre-established and follow-on questions are asked, responses documented, discussion encouraged, and conclusions reached.
- *Observe* – a real-time viewing by an assessor of PCI processes in operation, including all information system components of the PCI involved in creation, issuance, maintenance, and replacement of PIV Cards.
- *Test* – an evaluation of a component against a set of relevant PIV specifications using applicable test methods and metrics. For example, use of the NIST SP 800-85B test tool to verify conformance of the data model on the PIV Card with applicable sections of FIPS 201-1.

These methods are intended to provide the Assessor with sufficient, precise, accurate, and relevant evidence regarding an accreditation topic and focus area. One or more assessment methods may be required to determine if the PCI has satisfactorily met the objective outlined for that assessment procedure. Assessment results are used by the Assessor in determining the overall effectiveness of the PCI control.

Table 3 shows an example of the relationships among a PAT, an Accreditation Focus Area, several PCI controls, and their assessment procedures.

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Preparation and Maintenance of Documentation	DO-1	The organization develops and implements an operations plan according to the template in Appendix D. The operations plan references other documents as needed. **Assessment** *Determine if:* *(i.) the operations plan includes the relevant elements from the template in Appendix D (review);* *(ii.) the operations plan includes the list of PCI controls and included with each is the PCI control owner, how they were implemented and whether they are organization or facility specific (review);* *(iii.) for any documentation required but not included in the operations plan the name and location is provided (review);* *(iv.) the operations plan is reviewed and approved by designated officials within the organization (interview).*	SP 800-79-1, Section 2.11 – Accreditation Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for enrollment/identity proofing which are approved by the SAO. **Assessment** *Determine if*: *(i) the organization develops and documents written policy and procedures for identity proofing and enrollment (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	FIPS 201-1 2.2 PIV Identity Proofing and Registration Requirements

Table 3 - Sample PCI Controls with Assessment Procedures

Some organizations may need to customize their assessment procedures to meet their specific characteristics and needs. Assessment procedures may be specially tailored to match the characteristics of the PCI and its facilities. Assessment procedures may be augmented to ensure that a PCI control is assessed if it was customized to fit the special structure of the organization.

4.2 The Assessment Report

The Assessment Report is used to present the results of the assessment in a format that facilitates reviewing by the DAA. The DAA needs to evaluate the information in the Assessment Report in order to make a sound, credible decision regarding the residual risk of authorizing the operations of the PCI.

An Assessment Report template is provided in Appendix E. The report is organized according to the Accreditation Focus Areas for a PCI. For each PCI control, it must be documented what entity is responsible for the implementation of that control (the organization, another organization, or an external service provider) and if the PIC control is organizational or facility specific.

Card Issuance

C-1 – External Service Provider, Facility Specific

The issuer performs a 1:1 biometric match of the Applicant against the biometric included in the PIV Card or in the enrollment record. On successful match, the PIV Card shall be released to the applicant.

Summary of Assessment Findings – Partially Satisfied

Two-thirds of the assessments were satisfactory. The PCI requires that all applicants have a 1:1 biometric match performed before the card is released.

Assessment Deficiency and Potential Impact

The PCI Facility does not have a process documented for performing the 1:1 biometric match prior to releasing the personalized PIV Card to the applicant. Although the facility personnel appear to be knowledgeable about this requirement and the process was observed during card issuance, the lack of documentation may pose a problem if there is turnover in staff.

Recommendation

Update the operating procedures within the PCI Facility to include a clear description of this step in the process.

Figure 4 - Sample Assessment Report

During an assessment, the Assessor should report a result as being Satisfied, Partially Satisfied, or Not Satisfied. The Assessor then summarizes these results in the assessment report, indicating

the number of satisfied assessment procedures out of the total number of assessment procedures performed for that PCI control. If all assessment procedures are indicated as Satisfied, the PCI control itself can be marked as Satisfied. If all the assessment procedures are Not Satisfied, the PCI control is marked as Not Satisfied. Any other combination leaves the PCI control as Partially Satisfied.

In reporting the results of assessing a particular PCI control, the Assessor must consider the potential qualitative and quantitative results of the assessment procedures used (e.g., interviews, document reviews, observations, and tests). Multiple procedures provide for a more thorough, reliable, and complete evaluation of a PCI control. For example, a PCI's documentation may be incomplete, but if individuals are knowledgeable and the proper processes are observed to be in place, the Assessor may consider this as satisfactory. In this case the control may be marked as Partially Satisfied and left to the OIMO to update the PCI documentation as part of the corrective action plan.

Additionally, the Assessor must report all deficiencies of PCI controls that were scored as Partially Satisfied or Not Satisfied. The Assessor must use knowledge of FIPS 201-1 and understanding of security and privacy to identify the potential adverse impacts if the PCI control is not utilized satisfactorily. The DAA should use this input when deciding whether to authorize the operations of the PCI.

For each PCI control that has not been satisfactorily implemented, the Assessor must also provide a recommendation for replacing, repairing, or improving that PCI control. An Assessor must have the expertise to evaluate all potential deficiencies of PCI controls and make cogent recommendations for correction. These recommendations must be contained in the Corrective Action Plan (CAP). The OIMO must use the CAP to correct operational reliability problems found during the assessments.

The report should contain a brief but comprehensive summary of the assessment results. A table of the status of individual PCI controls should also be included. The Assessment Report template suggests a manner of compiling the assessment results going from the PCI control level to the Accreditation Focus Area and then the PCI Accreditation Topic (PAT) levels. An executive summary of the operational status of the PCI and its facilities, along with a statement of current and future reliability for senior organization officials who depend on the final report, should be included.

4.3 A Methodology for Performing an Assessment

This section defines a recommended assessment methodology for performing an accreditation of a PCI and its facilities under SP 800-79-1. This methodology relies on a seven-step process beginning with the selection of the PCI controls and concluding with generating the final assessment report to be submitted to the OIMO.

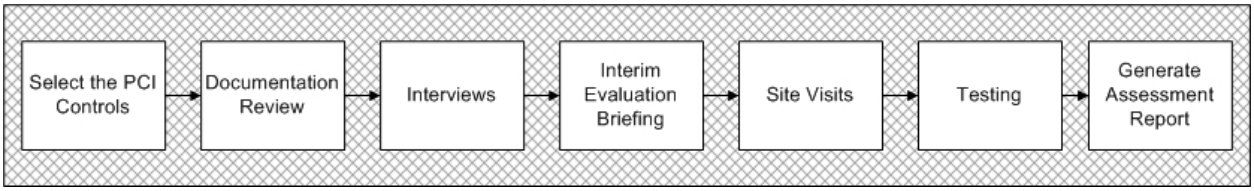

Figure 5 - An Assessment Methodology

4.3.1 Step 1: Select the PCI controls

During assessment initiation, the Assessor should first establish the accreditation boundary for this assessment. If the PCI and all its facilities are being assessed, all the PCI controls will need to be assessed. If the boundary does not contain the entire PCI, the assessor should then identify the PCI controls to be assessed within the restricted boundary. If the PCI and its facilities have already been assessed and are operating under a current Authorization to Operate (ATO) and the purpose of the assessment is to add a facility(s) to the accreditation letter, the Assessor can cite the previous assessment of PCI controls which apply at the organization level. There is no need to reassess these organization-level controls each time a PCIF is added to an ATO. However, all facility-level controls that apply to the new facility(s) will need to be assessed. If multiple PCIFs perform identical processes and have implemented identical controls, there is no need to assess the controls at every facility. In this case, the Assessor can choose a random sample of PCIFs to assess.

If PIV services have been out-sourced to an external provider, the Assessor should verify that the PCI controls applying to those services have been assessed and the reliability of the service provider has been found satisfactory. If the PCI controls have not been assessed by the external service provider, the Assessor should assess them in order for the DAA to issue an ATO. Even if the PCI has out-sourced its PCI services, all PCI controls that apply to the PCI must be assessed.

Following identifying the controls within the assessment boundary to be assessed, documentation review should commence.

4.3.2 Step 2: Perform Documentation Review

During this step, the Assessor should identify all documentation required of the PCI, and review the documentation received from the PCI. Reviewing previous PCI assessment reports and accreditation decisions is a good starting point. Previous assessments may not substitute for current assessments, but do provide a snapshot view of the PCI and highlight problems that existed in the past.

The main document to be reviewed is the operations plan. It describes all the policies, procedures, and processes of the PCI, and it should adhere to the template in Appendix D. Other documentation which should be reviewed includes:

- Letters of appointment;
- Interconnection Security Agreements (ISAs) and Memoranda of Understanding (MOUs) for all connections between a PCI's information systems and external information systems;

- Listing of all PIV service and function components used within the PCI;
- Privacy-related documentation;
- All standard forms utilized within the PCI;
- Documentation from each out-sourced service provider, such as its operating plan, support agreements, contracts, etc;
- Standard operating procedures for the PCIFs within the accreditation boundary for the PCI; and
- Signed accreditation letters under SP 800-37 for all information systems within the PCI.

The documentation review is to assess the PCI controls that are implemented via appropriate documentation. Many of these PCI controls have the assigned assessment method of Review, indicating a review of documentation is necessary.

The Assessor may report to the OIMO if any areas of non-conformance are found during the documentation review if this is authorized and directed by the Senior Authorizing Official (SAO). During this step, the Assessor should document all areas of non-conformance for later review.

4.3.3 Step 3: Perform Interviews

During this step, the Assessor should develop an interview list that includes individuals who fill the roles defined in this Special Publication. The Assessor may also want to interview individuals responsible for specific functions within the PCI and its facilities, such as enrollment/identity proofing and card activation/issuance managers. Interviews are an opportunity to clarify issues encountered during the documentation review and fill-in any gaps that may exist pertaining to how PCI controls have been implemented. During this step, the assessor should document all areas of non-conformance for later review.

4.3.4 Step 4: Interim Evaluation Briefing

After completion of Steps 2 and 3, a briefing should be scheduled with the DAA and OIMO (or, assessment team) to present the findings to-date. This briefing allows for the DAA and OIMO to gauge the current state of the assessment activity as well as provide feedback to the Assessor on the areas of non-conformance.

4.3.5 Step 5: Perform Site Visits

During this step, the assessor should perform on-site evaluations of the PCI and its facilities. Interviews that were not completed as part of Step 3 should be conducted with PCIF personnel to determine if they understand their day-to-day duties in the PCIF and are performing the defined assignments in accordance with the reviewed documentation.

In addition, the physical characteristics of the facility should be assessed to ensure that the facility-specific PCI controls are implemented in the manner described in the policies and procedures. Examples include verification that the proper signs have been displayed, as well as

ensuring that the correct forms are used when enrolling applicants and issuing PIV Cards to cardholders.

During the site visit, the Assessor should evaluate at least one demonstration of all the steps required to issue and maintain a PIV Card starting with sponsorship. There are a significant number of PCI controls that require observation of processes. Processes such as properly capturing fingerprints according to Table 2 in SP 800-76-1 require that the Assessor be on site to observe.

4.3.6 Step 6: Perform Testing

Once the site visits have been completed and a production version of the PIV Card produced, the Assessor should begin testing relevant components (e.g., PCI card stock, fingerprint readers, card readers/writers, software, communications) required by many PCI controls. Many of these tests focus on the PIV Card and the data elements therein. Assessors should prepare for these tests in advance. For example, have the SP 800-85B test tool prepared and ready for execution. In other cases, such as manually testing the facial image on the card, the Assessors should understand how the facial image must be stored on the card according to the Standard, and should have the expertise to extract the data from the card in order to test it.

4.3.7 Step 7: Generate Assessment Report

During this step, the Assessor should consolidate the results of the assessment steps, and develop the assessment report according to the template in Appendix E. In this report, the Assessor reports their findings for each PCI control, and then summarizes the findings according to the summary format of the report.

Of particular importance in the assessment report is a description of deficiencies with particular PCI controls, recommendations for addressing the deficiencies, and the impact to the organization if the deficiencies are not addresses. This final report is delivered to the OIMO. This report, combined with the updated operations plan, the CAP, and any SP 800-37 accreditation letters, makes up the accreditation package that the OIMO submits to the DAA.

5.0 ACCREDITATION

The accreditation of a PIV Card Issuer (PCI) consists of four phases: (i) Initiation; (ii) Assessment; (iii) Accreditation; and (iv) Monitoring. Each phase consists of tasks and sub-tasks that are to be carried out by the responsible officials (e.g., the Designated Accreditation Authority (DAA), Assessor, Organization Identity Management Official (OIMO), and PCI Facility (PCIF) Manager). Figure 6 provides a view of the accreditation phases including the tasks associated with each phase. A table of accreditation phases, tasks, sub-tasks, and the official responsible for each is provided in Appendix H.

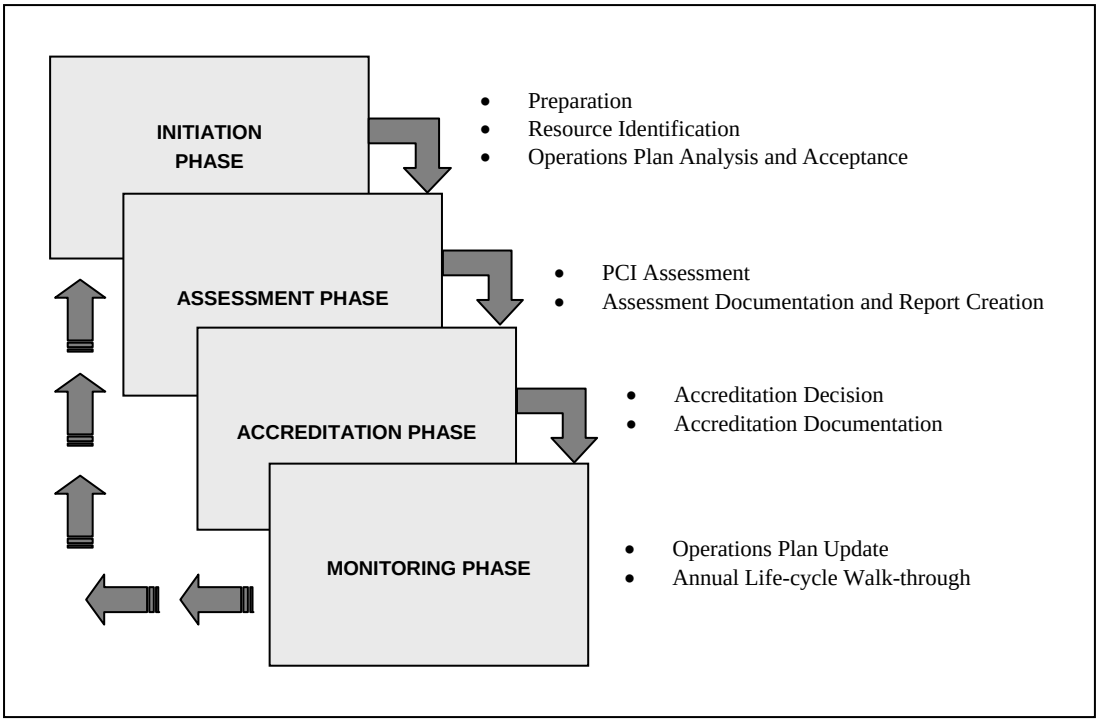

Figure 6 - Accreditation Phases

5.1 Initiation Phase

The Initiation Phase consists of three tasks: (i) preparation; (ii) resource identification; and (iii) operations plan analysis and acceptance. The primary purpose of this phase is to ensure that the PCI is prepared for the assessment, including having all the resources and documentation in place. The other purpose of this phase is to include the DAA early on in the process in order to assure success of the assessment and accreditation.

Task 1: Preparation

The objectives of this task are to prepare for accreditation by reviewing the PCI operations plan and confirming that the plan is consistent with Federal Information Processing Standard (FIPS) 201-1 and the template provided herein.

Subtask 1.1: Confirm that the PCI and its operations have been fully described and documented in the PCI's operations plan.

Responsibility: OIMO

Guidance: The PCI operation plan includes at a minimum the sections defined in the operations plan template in Appendix D. It is the OIMO's responsibility to ensure that the organization's PCI operations plan incorporates a complete and accurate description of the PCI's operations. If an external service provider is managing out-sourced functions and has them documented, the organization can incorporate this documentation in their internal operations plan by reference. In this case, the operations plan serves as pointer, guiding the reader to additional documentation and information.

Subtask 1.2: Confirm that the PCI's services and/or information systems have not been categorized as National Security.

Responsibility: OIMO

Guidance: Consult NIST Special Publication (SP) 800-59, *Guideline for Identifying an Information System as a National Security System*, to confirm that the applicability of the PCI's services and information systems are not related to National Security.

Subtask 1.3: Confirm that the PCI has documented in the operations plan its processes for the major functional areas including enrollment, issuance, maintenance, termination, re-issuance, and renewal.

Responsibility: OIMO

Guidance: FIPS 201-1, Sections 2.2 and 2.3 require the adoption and use of these processes. Two models (Role Based and System Based) are identified in FIPS 201-1 as satisfying the requirements.

Subtask 1.4: Confirm that processes followed at the PCI Facility are conducted in accordance with the policies and procedures specified in the PCI operations plan and are documented in Standard Operating Procedures.

Responsibility: OIMO, PCIF Manager

Guidance: Even though PCI Facilities may be following requirements from FIPS 201-1, their processes need to be consistent with those prescribed by the PCI's operations plan and documented in Standard Operating Procedures.

Task 2: Resource Identification

The objectives of the resource identification task are to— (i) identify and document the resources required for assisting with the assessment; and (ii) prepare a plan of assessment activities indicating the proposed schedule and key milestones.

Subtask 2.1: Identify the Senior Authorizing Official (SAO), DAA, Privacy Official (PO), Assessor(s), and other officials at the facility level, such as enrollment/identity

proofing, card production, card activation/issuance and maintenance PCI personnel who can provide requested assessment information to the Assessor. Notify these individuals of the upcoming assessment, and inform them of the need for their participation during the process.

Responsibility: OIMO

Guidance: The creation and assignment of these roles must be done early in the implementation of a PCI. If these roles have not been delegated, individuals must be selected and notified of their responsibilities.

Subtask 2.2: Determine the accreditation boundary.

Responsibility: OIMO; DAA

Guidance: The accreditation boundary determines the target of the assessment. In preparation for a PCI assessment, the OIMO and DAA should identify which PCIFs and external service providers are to be included. The PCI must always be included in the accreditation boundary. An organization may want to include a subset of those PCIFs that are ready to operate; other facilities can be assessed at a later date. External service providers must be included in the accreditation boundary. This ensures that functions performed and processes managed by the external service provider are considered during the accreditation process.

Subtask 2.3: Determine the resources and the time needed for the accreditation of the PCI, and prepare a plan of execution.

Responsibility: OIMO; DAA

Guidance: The level of effort required for assessment depends on numerous factors— (i) the size the PCI; (ii) the location and number of its facilities; (iii) the level of outsourcing utilized by the PCI; and (iv) the number of cards being, or to be, issued. By examining factors that could influence the complexity of the assessment, the organization can make informed judgments about the size of the assessment team, the resources needed to support the assessment, and the time-frame for completing it.

Task 3: Operations Plan Analysis and Acceptance

The objectives of the operations plan analysis and acceptance task are to— (i) perform an analysis of whether the requirements of FIPS 201-1 have been implemented; (ii) obtain an independent analysis of the PCI operations plan and revise as needed; and (iii) obtain acceptance of the plan by the DAA prior to conducting an assessment of the PCI controls.

Subtask 3.1: Review the list of required PCI controls documented in the organization's operation plan and then confirm that they have been implemented properly.

Responsibility: DAA; OIMO

Guidance: Since the PCI controls serve as the basis for the assessment, a review the PCI's documentation and operations plan to identify the controls that should be implemented before investing time in assessment activities such as interviews or testing. The operations plan must document each PCI control, whether it is organization or facility specific, the owner of the PCI control, and how the PCI control should be implemented.

Subtask 3.2: Analyze the PCI operations plan to determine if there are deficiencies in satisfying all the policies, procedures, and other requirements in FIPS 201-1that could result in a Denial of Authorization To Operate (DATO) being issued. After discussing the discovered deficiencies in the documentation and operations plan with the OIMO, the organization may still want to continue with the assessment. If so, the DAA must authorize the continuation of the assessment.

Responsibility: OIMO, DAA

Guidance: The operations plan should adequately specify the policies, procedures, and processes of the PCI so that subsequent to an initial review, deficiencies that could lead to an eventual DATO may be identified for the PCI.

Subtask 3.3: Verify that the PCI operations plan is acceptable.

Responsibility: DAA

Guidance: If the PCI operations plan is deemed acceptable, the DAA should authorize the accreditation processes to advance to the next phase. Acceptance of the PCI operations plan signifies that the resources required to initiate and complete the accreditation activities may be deployed.

5.2 Assessment Phase

The Assessment Phase consists of two tasks— (i) PCI control assessment; and (ii) assessment documentation. The purpose of this phase is to determine the extent to which the requirements of FIPS 201-1 are implemented correctly, operating as intended, and producing the desired outcomes. This phase also specifies actions to be taken to correct all identified deficiencies. An analysis of the impact of identified deficiencies that cannot be corrected or mitigated efficiently on the reliable operation of the PCI should be conducted and documented. Successful completion of this phase should provide the DAA with the information needed to make an appropriate accreditation decision.

Task 4: PCI Control Assessment

The objectives of this task are to— (i) initiate an assessment of the PCI controls; (ii) conduct the assessment; and (iii) document the results of the assessment. After the Assessor verifies the acceptability of all relevant documentation including the operations plan, previous assessments,

and federal laws, regulations, standards, directives, etc., PCI control assessment should commence. The assessor should schedule interviews, schedule real-time observations of PCI processes, initiate all needed testing of the PIV Card and PCI information system components, and plan other required assessment activities. Once the Assessor has gathered the results of the assessment procedures, recommendations on corrective actions for discovered deficiencies may be made.

Subtask 4.1: Review the suggested and selected assessment methods for each PCI control in preparation for the assessment.

Responsibility: Assessor

Guidance: The Assessor(s) should review the selected assessment procedures in order to plan and coordinate activities for the assessment. For instance, if a particular PCI control requires observation of a particular process, the Assessor will need to schedule this activity in a timely fashion after coordinating it with the PCI's or PCIF's management. The Assessor, as directed by the DAA, may supplement the assessment methods and procedures recommended in these guidelines. Assessment methods and procedures may be created or tailored for a particular PCI.

Subtask 4.2: Assemble all documentation and supporting materials necessary for the assessment of the PCI; if these documents include previous assessments, review the findings and determine if they are applicable to the current assessment.

Responsibility: OIMO; Assessor

Guidance: The OIMO assists the Assessor in gathering all relevant documents and supporting materials from the organization that will be required during the assessment of the PCI. Central to this effort is the operations plan. The PCI's operations should be completely described in the operations plan. The operations plan may include by reference, or point to, the supporting materials. In this case, the OIMO will need to gather this supporting material for the Assessor. When previous assessments exist, including the one on which the current Authorization to Operate (ATO) is based, the Assessor must review the results. The Assessor may satisfy some of the PCI control assessment requirements by reviewing and referencing the assessment report(s).

Subtask 4.3: Assess the required PCI controls using the prescribed or recommended assessment procedures found in Appendix G.

Responsibility: Assessor

Guidance: The Assessor performs the assessment procedures selected for each PCI control to assess if the PCI controls have been implemented correctly, are operating as intended, and producing the desired outcomes. If the Assessor is

assessing both a PCI and specific PCIFs, organization and the facility-specific PCI controls are assessed respectively. If the Assessor is only assessing a PCIF(s), and the PCI is already accredited under an ATO, the assessment results of the organizational PCI controls can be used. The Assessor should focus on assessing the facility-specific PCI controls which apply to the facility(s).

Subtask 4.4: Prepare the assessment report.

Responsibility: Assessor

Guidance: The assessment report contains— (i) the results of the assessment; (ii) recommendations for correcting deficiencies; and (iii) the residual impact to the organization of any deficiency that cannot be corrected or mitigated. The assessment report should become part of the final accreditation package along with the PCI operations plan and corrective actions plan (CAP). The assessment report is the Assessor's statement of the results of analyzing and evaluating the PCI controls as implemented by the PCI. The sample assessment report template in Appendix E should be used as the basis for the assessment report.

Task 5: Assessment Documentation

The assessment documentation task (i) provides the assessment findings and recommendations to the OIMO; (ii) recommends revision of the PCI's operation plan as needed; (iii) prepares the CAP (including milestones); and (iv) assembles the accreditation package. The OIMO has an opportunity to reduce or eliminate deficiencies in the PCI's operations prior to the assembly of the accreditation package and submission to the DAA. This is accomplished by implementing the corrective actions recommended by the Assessor.

Subtask 5.1: Provide the OIMO with the assessment report.

Responsibility: Assessor

Guidance: The OIMO relies on the expertise, experience, and judgment of the Assessor to (i) provide recommendations on how to correct deficiencies in the planned or performed operations; (ii) and to understand the potential impacts of those deficiencies. The OIMO may choose to act on selected recommendations of the Assessor before the accreditation package is finalized. To optimize the utilization of resources organization-wide, any actions taken by the OIMO prior to the final accreditation decision must be coordinated with the DAA. The Assessor reviews any changes made in response to the corrective actions and revises the assessment report as appropriate. A sample Assessment Report format is included in Appendix E.

Subtask 5.2: Revise the PCI operations plan (if necessary) and implement its new provisions.

Responsibility: OIMO

Guidance: The revised PCI operations plan must include all changes made in response to recommendations for corrective actions from the Assessor.

Subtask 5.3: Prepare the Corrective Actions Plan.

Responsibility: OIMO

Guidance: The CAP, one of the three primary documents in the accreditation package, describes actions that must be taken by the OIMO to correct deficiencies identified in the Assessment phase. The CAP identifies— (i) the tasks to be accomplished; (ii) the resources required to accomplish the tasks; and (iii) scheduled completion dates for the tasks.

Subtask 5.4: Assemble the accreditation package and submit to the DAA.

Responsibility: Assessor; OIMO

Guidance: The Assessor is responsible for the assembly and compilation of the accreditation package with inputs from the OIMO. The accreditation package should contain: (i) the final assessment report; (ii) the CAP; (iii) the revised PCI operations plan; and (iv) the SP 800-37 accreditation letters for all information systems within the PCI. The Assessor and OIMO may wish to consult other key organization participants (e.g., the PO) prior to submitting the final accreditation package to the DAA. The accreditation package can be submitted in either paper or electronic form. The contents of the accreditation package must be protected in accordance with organization policy.

5.3 Accreditation Phase

The Accreditation Phase consists of two tasks— (i) making an appropriate accreditation decision; and (ii) completing the accreditation documentation. Upon completion of this phase, the OIMO will have— (i) an authorization to operate the PCI services defined in its operations plan; (ii) an interim authorization to operate under specific terms and conditions; or (iii) a denial of authorization.

Task 6: Accreditation Decision

The accreditation decision task determines if the assessment phase has been satisfactorily completed so that a recommendation concerning operation of the PCI can be made with assurance. The DAA, working with the Assessor, reviews the assessment package, the identified and uncorrected or un-correctable deficiencies, the potential impacts on each organization using the PCI's services, and the CAP in determining the final risk to the organization(s) and the acceptability of that risk in light of the organization's mission.

Subtask 6.1: Determine the risk to an organization's operations, assets, or individuals based on the PCI's deficiencies, the impacts of those deficiencies, and the CAP and perform a final assessment review.

Responsibility: DAA

Guidance: The DAA receives the final accreditation package from the Assessor. The DAA judges which deficiencies are of greatest concern to the organization and which can be tolerated without creating unreasonable organization-level risk. The CAP is also considered in determining the risk to the organization in terms of when and how the OIMO intends to address the known deficiencies. The DAA may consult the OIMO, Assessor, or other organization officials before making the final risk determination.

Subtask 6.2: Determine if the risk to the organization's operations, assets, or potentially affected individuals is acceptable, that the PCI controls have been adequately assessed, and prepare the final accreditation decision letter.

Responsibility: DAA

Guidance: The DAA must consider many factors when deciding that a PCI can create and issue PIV Cards reliably and if the risk to the organization and its mission, assets, and individuals is acceptable. The issuance of a Federal government-wide PIV Card is the foundation for the card holder to access many government physical and logical resources. Any uncorrected deficiency in a primary PCI service or function could lead to unauthorized people gaining access or authorized people not gaining the needed access. In addition to the security risks, there are significant privacy concerns regarding personal information that has to be stored, exchanged, and processed in accordance with the provisions of HSPD-12. The DAA must carefully analyze how failures to conform to FIPS 201-1 requirements could impact the organization's mission. Such failures could lead to major adverse impacts on security and privacy within the organization and across the entire Federal government.

If, after analyzing the results of PCI reliability assessment, the DAA deems that the organization-level risk is acceptable, the PCI and its approved facilities are accredited without any restrictions or limitations and an ATO should be issued.

If, after analyzing the results, the DAA deems that the organization-level risk is unacceptable, but there is an important mission requiring the PCI's operation, an interim authorization to operate may be issued. The interim authorization to operate limits operation of the PCI and its facilities an organization-defined period of time (maximum of 3 months), includes specific terms and conditions for operations, and includes a required time frame for completion of all recommended actions in the CAP. A detailed CAP is to be submitted by the OIMO and Assessor and approved by the DAA prior to the interim authorization to operate taking effect. The PCI is not considered accredited during this period. The OIMO is

responsible for completing the corrective actions identified in the CAP and resubmitting an updated accreditation package upon completion of those actions.

If, after assessing the results of the assessment, the DAA deems that the organization-level risk is unacceptable, the PCI is denied an authorization for operation and not accredited.

The DAA prepares the final accreditation decision letter. The letter includes the accreditation decision, the rationale for the decision, the terms and conditions for the PCI's operation, and required corrective actions, if appropriate. The accreditation decision letter states whether the PCI is— (i) authorized to operate; (ii) authorized to operate on an interim basis under strict terms and conditions; or (iii) not authorized to operate. The supporting rationale provides the rationale for the DAA's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions that must be followed. The accreditation letter is included in the final accreditation package. The contents of the accreditation package must be protected appropriately in accordance with organization policy.

Task 7: Accreditation Documentation

The accreditation documentation task includes— (i) completing and transmitting the final accreditation package to the appropriate individuals and organizations; and (ii) updating the PCI's operations plan.

Subtask 7.1: Provide copies of the final accreditation package including the accreditation decision letter, in either paper or electronic form, to the OIMO and any other organization officials having interests, roles, or responsibilities in the PCI.

Responsibility: DAA

Guidance: The accreditation package including the accreditation decision letter should be transmitted to the OIMO. Upon receipt of the accreditation decision letter and accreditation package, the OIMO should review the authorization and its terms and conditions. The original accreditation package should be kept on file by the OIMO. The DAA should retain copies of the decision letter and accreditation package. The accreditation package must be appropriately safeguarded and stored, whenever possible, in a centralized organization filing system to ensure accessibility. The accreditation package should be available to authorized auditors and oversight organizations upon request. The accreditation package should be retained in accordance with the organization's records retention policy. The PCI and specific facilities are accredited for a maximum of three (3) years from the date of the ATO. After the period ends re-accreditation must be performed.

Subtask 7.2: Update the PCI's operations plan.

Responsibility: OIMO

Guidance: The operations plan must be updated to reflect all changes made as the result of assessment and accreditation. All conditions of PCI operations that are set forth in the accreditation decision must also be noted in the plan.

5.4 Monitoring Phase

The Monitoring Phase consists of three tasks— (i) operations plan maintenance; (ii) PIV Card life-cycle walk-through; and (iii) communications with the DAA. Based on the importance of reliably creating and issuing PIV Cards, it is imperative that once the accreditation is completed the PCI be monitored to ensure that policies, procedures, and processes remain in effect as originally intended. There can be significant changes in a PCI's policies, management, operations personnel, and available technology during a three-year ATO. These changes must be monitored in order that the organization minimizes exposing itself to a security or privacy threat existing or arising in the PCI. For example, if there is significant staff turnover in the PCI, the organization must be sure that the new PCI staff is enrolling card applicants and issuing cards using the same reliable processes previously approved.

In order to facilitate monitoring of a PCI without undue burden in activities and paperwork, only two activities are required during this phase: maintenance of the operations plan and annual life-cycle walk-through of PCI operations. The latter entails reviewing all the services and functions of a PCI and its facilities for continued reliability in performing them. The annual walk-through should cover a PIV Card's life-cycle from sponsorship to maintenance. Observation of this full life cycle of a card should ensure that all processes are still reliably operating as assessed during the accreditation.

Task 8: Operations Plan Update

A PCI's operations plan is the primary description of what and how PIV Card Issuing services are provided. It is essential that this document be updated as changes occur in the PCI's operations. The PCI management will be able to analyze the impact of changes as they occur and will be significantly better prepared when re-accreditation in required.

Subtask 8.1: Document all relevant changes in the PCI within the operations plan.

Responsibility: OIMO

Guidance: In addition to the policies, procedures, and processes that must be documented if changes to them are made, the organization should update the operations plan if changes to the PCI information system, the PIV Card, privacy policies, roles and responsibilities, or PCI controls are changed.

Subtask 8.2: Analyze the proposed or actual changes to the PCI and determine the impact of such changes.

Responsibility: OIMO

Guidance: If the results of the impact analysis indicate that changes to the PCI could affect the reliability of the PCI's operations, the changes and impact on the PCI must be reported to the DAA, corrective actions must be initiated, and the CAP must be updated. In instances where major changes have occurred, it is recommended that an assessment be performed on the changed PCI, and accreditation of the PCI is repeated in its entirety if the DAA requests it.

Task 9: Life-cycle Walk-through

The Life-cycle Walk-through is a monitoring activity to be performed initially by the PCI when its PIV Card issuing services begin, and annually thereafter. The OIMO designates an organization official to observe and review the entire life-cycle of a PIV Card. This walk-through should provide a good snapshot of the PCI's operations and reliability at a point in time. By walking through the PIV Card life-cycle from sponsorship to issuance to maintenance, the operations of the PCI can be examined as an integrated entity. During the Life-cycle Walk-through, the organization official should observe all processes involving the PIV Card, comparing them against the requirements defined in the PCI controls. This activity should be performed every year after each accreditation until re-accreditation begins. All identified deficiencies in reliable operations should be sent to the DAA for review and analysis. Any potential impact to the reliability of the PCI's operations and risk to the organization should be documented and presented to the AIMO and the DAA.

Subtask 9.1: An organization official observes all the processes involved in getting a PIV Card, including those going from sponsorship to maintenance. The official should observe each process and compare its controls against the applicable list of required PCI controls. If a PCI has several facilities, this process should be repeated using randomly selected of PCIFs.

Responsibility: OIMO, selected organization official

Guidance: An unannounced organization official should be selected to perform the walk-through and be sponsored as a new employee to receive a PIV Card. In order to process the sponsorship request, the organization official should participate as a new employee by completing all the steps required for receiving a PIV Card. During each step, the official should be monitored by the OIMO, who will observe each step of issuing a PIV Card and compare it against the required steps and their associated PCI controls. PIV Card maintenance processes must be included as well, including having the card terminated, reissued, or renewed. An annual walk-through is required until re-accreditation is initiated.

Subtask 9.2: The results of the life-cycle walk-through are summarized in a report to the DAA. Deficiencies must be highlighted along with corrective actions that must be done to correct any deficiencies.

Responsibility: OIMO, DAA

Guidance: The OIMO should document all PCI processes involved in providing a PIV Card to the organization official. The results of the life-cycle walk-through

should be recorded in the assessment report template in Appendix E. All deficiencies should be described and a plan for correcting each deficiency should be documented. The DAA should decide if any deficiency is significant enough to require a change of the PCI's authorization to operate status.

APPENDIX A: REFERENCES

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974*, December 31, 1974 (effective September 27, 1975).
(Available at http://www.archives.gov/research_room/foia_reading_room/privacy_act/privacy_act.html.)

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002*, December 17, 2002.
(Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf.)

Committee for National Security Systems, Instruction 4009, *National Information Assurance Glossary*, Revised May 2003.
(Available at http://staff.washington.edu/dittrich/center/4009.pdf.)

Executive Office of the President, Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953.
(Available at http://www.archives.gov/federal-register/codification/executive-order/10450.html.)

Executive Office of the President, Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
(Available at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.)

Federal Identity Credentialing Committee, *Federal Identity Management Handbook*, Version 0.1, December 2005.
(Available at http://www.cio.gov/ficc/documents/FederalIdentityManagementHandbook.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Draft Federal Information Processing Standards Publication 140-3, *Security Requirements for Cryptographic Modules*, July 2007.
(Available at http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-140-3.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
(Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Security Controls for Federal Information Systems*, March 2006.
(Available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006.
(Available at http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Version 2.0, May 2004.
(Available at http:/csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, December 2006.
(Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
(Available at http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-73-2, *Interfaces for Personal Identity Verification*, October 2007.
(Available at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-73--2.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.
(Available at http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, August 2007.
(Available at http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, April 2006.
(Available at http://csrc.nist.gov/publications/nistpubs/800-85A/SP800-85A.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006.
(Available at http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, June 2007.
(Available at http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29_2007-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Draft Interagency Report 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems*, September 2007.
(Available at http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7328.)

United States Office of Management and Budget, *Circular No. A-130 Revised*, Appendix III, Security of Federal Automated Information Resources, February 1996.
(Available at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.)

APPENDIX B: GLOSSARY AND ACRONYMS

Terms/Acronyms used in this document	Definition or explanation of term; expansion of acronym
Access Control	The process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Accreditation (as applied to a PCI)	The official management decision of the Designated Accreditation Authority to authorize operation of a PCI after determining that the PCI's reliability has satisfactorily being established through appropriate assessment processes.
Accreditation Package	The results of assessment and supporting documentation provided to the Designated Accreditation Authority to be used in the accreditation decision process.
Agency	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Applicant	An individual applying for a PIV Card/credential. The Applicant may be a current or prospective Federal employee or contractor.
Assessment (as applied to a PCI)	Assessment in this context means a formal process of assessing the implementation and reliable use of PCI controls using various methods of assessment (e.g., interviews, document reviews, observations) that support the assertion that a PCI is reliably meeting the requirements of FIPS 201-1.
Assessment Method	A focused activity or action employed by an Assessor for evaluating a particular PCI control.
Assessment Procedure	A set of activities or actions employed by an Assessor to determine the extent that a PCI control is implemented and used by a PCI.
Assessor	The individual, group, or organization responsible for conducting assessment activities under the guidance and direction of a Designated Accreditation Authority.
ATO	Authorization to Operate; One of three possible decisions concerning a PCI made by a Designated Accreditation Authority after all assessment activities have been performed stating that the reliability of the PCI is accredited and the PCI is authorized to perform specific PIV Card services.
Authorizing Official	See Designated Accreditation Authority
CAP (or Corrective Action	Corrective Action Plan of a PCI for removing or reducing

Terms/Acronyms used in this document	Definition or explanation of term; expansion of acronym
Plan)	deficiencies or risks during PCI operations. The document that identifies corrective action tasks that need to be performed in order to obtain or sustain accreditation.
Card Activation/Issuance	A processes including the procurement of FIPS-approved blank identity cards, initialing them using appropriate software and data elements for identity verification and access control applications, personalization of the cards with the identity credentials of authorized subjects, and delivery of the personalized cards to the authorized subjects along with appropriate instructions for protection and use.
Component	An element, such as a fingerprint-input station or card reader within the PCI for which FIPS 201-1 makes specific requirements.
Credential	Evidence attesting to one's right to credit or authority; in FIPS 201, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
DAA	Designated Accreditation Authority (also called an Authorizing Official); A senior organization official that has been given the authorization to accredit the reliability of a PCI.
DATO	Denial of Authorization to Operate; issued by a DAA to a PCI that is not accredited as being reliable in the issuance of PIV Cards.
Enrollment/Identity Proofing	The processes including (i) identity proofing and (ii) making a person's identity known to the PCI information system by associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the PCI information system. Enrollment is necessary in order to initiate other processes such as adjudication, card issuance and maintenance that are necessary to issue and maintain a PIV Card.
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive; HSPD-12 established the policy for which FIPS 201 was developed.
IATO	Interim Authorization to Operate a PCI performing specified services (e.g., enrollment/identity proofing, card production, card activation/issuance and maintenance).
Identification	The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar

Terms/Acronyms used in this document	Definition or explanation of term; expansion of acronym
	persons or items.
Identifier	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
Identity Proofing	Verifying the claimed identity of an Applicant by authenticating the identity source documents provided by the Applicant.
IIF	Information in Identifiable Form; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. [E-Gov]
ITL	Information Technology Laboratory
Maintenance	The process of managing PIV Cards once they are issued. It includes termination, renewal and re-issuance.
National Security System	Any information system used or operated by an organization or its contractor: (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding an information system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
NIST	National Institute of Standards and Technology
OIMO (or Organization Identity Management Official)	The individual responsible for overseeing operations of a PCI in accordance with FIPS 201-1 and for performing the responsibilities specified in this guideline.
OMB	Office of Management and Budget
PCI	PIV Card Issuer
PCI information system	A computer-based system used by a PCI to perform the functions necessary for PIV Card issuance as per FIPS 201-1.
PCIF	PCI Facility

Terms/Acronyms used in this document	Definition or explanation of term; expansion of acronym
PIV	Personal Identity Verification as specified in FIPS 201-1.
PIV Card	The physical artifact (e.g., identity card, "smart" card) issued to an Applicant by a PCI that contains stored identity markers or credentials (e.g., photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
PO	Privacy Official
Risk	The level of potential impact on organization operations (including mission, functions, image, or reputation), organization assets, or individuals of a threat or a given likelihood of that threat occurring.
SAO	Senior Authorizing Official
SOP	Standard Operating Procedures
SOR	A system of records is a group of records under the control of a Federal agency which contains a personal identifier (such as a name, date of birth, finger print, Social Security Number, Employee Number, etc.) and one other item of personal data (such as home address, performance rating, blood type, etc.) from which information is retrieved by a personal identifier.
SORN	The Privacy Act requires each agency to publish notice if its systems of records in the Federal Register. This is called a System of Record Notice (SORN).
SP	Special Publication
Sponsor	An individual who can act on behalf of an organization to request that a PIV Card be issued to an Applicant after appropriate identity authentication and background checks.

APPENDIX C: PCI READINESS REVIEW CHECKLIST

The readiness review checklist may be used by a PCI preparing for assessment and accreditation by an assessment team. The checklist may also be used to validate that the PCI has collected all relevant documentation, identified appropriate individuals with knowledge of the PCI and made them available, and provided access to the PCI to the assessment team.

Activity	Completed?	Comments
• Identify an independent assessment team to assess the PCI.		
• Determine the accreditation boundary.		
• Establish the scope and objectives of the assessment.		
• Determine the level of effort and resources necessary to carry out the assessment.		
• Establish the time-frame to complete the assessment and identify key milestone decision points.		
• Notify key officials and any out-sourced providers of the impending assessment.		
• Validate that the PCI operations plan is complete and includes all the required information.		
• Ensure that the necessary roles within the PCI have been designated.		
• Validate that implementation and management responsibility for PCI controls have been accurately assigned.		
• Make sure that the information systems utilized by the PCI have been certified and accredited to operate in accordance with SP 800-37.		
• Ensure that the following documentation has been developed and can be made available to the assessment team: (i) PCI Operations plan (ii) Results from any past assessment and accreditation decisions for the PCI (iii) Letters of appointment (if any) (iv) Interconnection Security Agreement		

Activity	Completed?	Comments
(ISA) and Memorandums of Understanding (MOU) for each connection between a PCI information systems and external information system. (v) Listing of all HSPD-12 components used within the PIV system (vi) Privacy-related documentation (vii) All forms utilized within the PCI (viii) Documentation from out-sourced providers (ix) Standard operating procedures for the PCI Facilities within the accreditation boundary for the PCI (x) Signed accreditation letter under SP 800-37 for each information system within the PCI		
• Live processes for the assessment team to observe.		
• A sample of PIV Cards produced by the PCI.		

APPENDIX D: PCI OPERATIONS PLAN TEMPLATE

I. Background

II. Purpose

III. Applicable Laws, Directives, Policies, Regulations & Standards Roles and Responsibilities

IV. Assignment of Roles

V. PCI Description

VI. PCI Facility Description and Locations

VII. PCI Management

a. Outsourcing
b. Facility management
c. Staffing
d. Training
e. Procurement

VIII. Policy and Procedure Descriptions

a. Enrollment/Identity Proofing
b. Card Production
c. Card Activation/Issuance
d. Maintenance
    i. Card Termination
    ii. Card Renewal
    iii. Card Re-issuance
b. Temporary Badges

II. PCI Information System (s) Description

a. Architecture
b. Interconnections and Information Sharing
c. Information System Inventory
d. Public Key Infrastructure
e. SP 800-37 C&A Information

III. Card Personalization & Production

a. Policy and Process Descriptions
b. PIV Card Graphical Topology
c. PIV Card Electronic Security
d. Expiration Date Requirements
e. Card Inventory Management
f. Card Reporting Requirements

IV. PCI controls

a. Name of PCI Control
b. PCI Control Owner
c. Organization/Facility Specific
d. How the PCI control is implemented

Appendix A - Memorandums of Appointment

Appendix B - Privacy Requirements

a. Privacy Policy
b. Privacy Impact Assessment
c. System of Record Notice
d. Privacy Act Statement/Notice
e. Rules of Conduct
f. Privacy Processes
    i. Requests to review personal information
    ii. Requests to amend personal information
    iii. Appeal procedures
    iv. Complaint procedures

APPENDIX E: ASSESSMENT REPORT TEMPLATE

Below is a template to use when generating the assessment report. This is to be completed for each PCI control. An example using a specific PCI control follows.

Accreditation Focus Area

PCI Control Number— (PCI Control Owner), (Organization or Facility Specific)

PCI Control Description

Summary of Assessment Findings— (Satisfied, Partially Satisfied, Not Satisfied)

(Number of Assessments Satisfactory out of Total Number of Assessments), (Description of findings)

Assessment Deficiency and Potential Impact

Recommendation

Card Activation/Issuance Process

AI-7 – External Service Provider, Facility Specific

The issuer performs a 1:1 biometric match of the Applicant against the biometric included in the PIV Card or in the enrollment record. On successful match, the PIV Card shall be released to the applicant.

Summary of Assessment Findings – Partially Satisfied
Two-thirds assessments were satisfactory. The PCI is requiring that all applicants have a 1:1 biometric match before the card is released.

Assessment Deficiency and Potential Impact
This process is not documented clearly enough in the operations plan. Although personnel are knowledgeable about this requirement and it was observed during card issuance, the lack of documentation could be a problem if there is turnover in staff.

Recommendation
Update the issuance process within the operations plan to include a clear description of this step in the process.

Summary Report Template

PAT (%Satisfied, % Partially Satisfied, % Not Satisfied)

For each Accreditation Focus Area

(%PCI controls Satisfied, % Partially Satisfied, % Not Satisfied)

(% Examine Assessments Satisfied, % Interview Assessments Satisfied, % Observe Assessments Satisfied)

APPENDIX F: SAMPLE TRANSMITTAL AND DECISION LETTERS

Sample Assessment/Accreditation Package Transmittal Letter

From: OIMO Date:

To: Designated Accreditation Authority (DAA)

Subject: PCI Accreditation Package for [PCI]

An assessment of the [PCI NAME] located at [PCI Location and PCIF Locations] has been conducted in accordance with NIST Special Publication (SP) 800-79-1, *Guidelines for the Accreditation of PIV Card Issuers* and the [ORGANIZATION] policy on PCI accreditation. The attached accreditation package contains— (i) the PCI operations plan; (ii) the assessment report; (iii) a corrective action plan (CAP); and (iv) An SP 800-37 accreditation letter for each information system within the PCI.

The PCI operations plan, its policies, procedures and processes have been assessed by [ASSESSOR] using the assessment methods and procedures defined in SP 800-79-1 and specified in the assessment report to determine the extent to which the requirements under HSPD-12 and FIPS 201-1 are exhibited. The CAP describes the corrective actions that we plan to perform to remove or reduce any remaining deficiencies detected in the PCI's operations.

Signature

Title

Sample Accreditation Decision Letter (Authorization to Operate)

From: Designated Accreditation Authority Date:

To: OIMO

Subject: Accreditation Decision for [OIMO]

After reviewing the results of the accreditation package of the [PCI], I have determined that the PCI's policies, procedures and processes are in compliance both with FIPS 201-1 and related documents and organization's own policies, regulations and standards. Accordingly, I am issuing an *authorization to operate* (ATO) the PCI's services. The PCI is accredited without any significant restrictions or limitations. This accreditation is my formal declaration that the requirements of HSPD-12 are being satisfied by the PCI.

This ATO also applies to facilities under the PCI. Included is a list of facilities authorized to operate under this accreditation decision.

This accreditation and ATO will remain in effect for 3 years from the date of this letter if— (i) all required documentation is updated annually; (ii) a life-cycle walk-through is completed annually and the results sent to me within thirty (30) days of completion; (iii) no deficiencies are identified during the walk-through that would increase the risk to the organization's mission.

A copy of this letter with all supporting accreditation documentation should be retained in accordance with the organization's record retention schedule.

Signature

Title

Sample Accreditation Decision Letter (Interim Authorization to Operate)

From: Designated Accreditation Authority Date:

To: OIMO

Subject: Accreditation Decision for [PCI]

After reviewing the results of the assessment of the [PCI], I have determined that the PCI does not satisfy the requirements identified in HSPD-12, FIPS 201-1 and related documents. However, I have determined that there is an overarching need for the PCI to provide the needed services due to mission necessity and other considerations. Accordingly, I am issuing an *interim authorization to operate* (IATO) the PCI's services. Operation of the PCI must be performed in accordance with the enclosed terms and conditions during the IATO period. The PCI is *not* considered accredited during the IATO period.

This IATO also applies to facilities under the PCI. Included is a list of facilities authorized to operate during this interim period.

This interim authorization to operate is valid for a maximum of [not to exceed three] months. This interim authorization will remain in effect as long as— (i) the required status reports for the PCI are submitted to this office every month; (ii) the problems or deficiencies reported from the accreditation do not result in additional risk that is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating the deficiencies in accordance with the corrective action plan (CAP). At the end of two IATO periods, the PCI must either accredit and authorized to operate or the authorization for further operation will be denied. This office will review the CAP submitted with the accreditation package during the IATO period and monitor progress on removal or reduction of concerns and discrepancies before re-accreditation is initiated.

A copy of this letter and all supporting accreditation documentation should be retained in accordance with the organization's record retention schedule.

Signature

Title

Sample Accreditation Decision Letter (Denial of Authorization to Operate)

From: Designated Accreditation Authority Date:

To: OIMO

Subject: Accreditation Decision for [OIMO]

After reviewing the results of the assessment of the [PCI] and the supporting evidence provided in the associated accreditation package, I have determined that the requirements from HSPD-12, FIPS 201-1 and related standards are not being exhibited by the PCI. Accordingly, I am issuing a denial of authorization to operate (DATO) the PCI or its facilities. The PCI is *not* accredited and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED].

The corrective action plan (CAP) is to be pursued immediately to ensure that proactive measures are taken to correct the deficiencies found during the assessment. Re- accreditation is to be initiated at the earliest opportunity to determine the effectiveness of correcting the deficiencies.

A copy of this letter with all supporting accreditation documentation must be retained in accordance with the organization's record retention schedule.

Signature

Title

APPENDIX G: PCI CONTROLS AND ASSESSMENT PROCEDURES

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Preparation and Maintenance of Documentation	DO-1	The organization develops and implements an operations plan according to the template in Appendix D. The operations plan references other documents as needed. **Assessment** *Determine if:* *(i) the operations plan includes the relevant elements from the template in Appendix D (review);* *(ii) the operations plan includes the list of PCI controls and included with each is the PCI control owner, how they were implemented and whether they are organization or facility specific (review);* *(iii) for any documentation required but not included in the operations plan the name and location is provided (review);* *(iv) the operations plan is reviewed and approved by designated officials within the organization (interview).*	SP 800-79-1, Section 2.11 – Accreditation Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for enrollment/identity proofing which are signed off by the head of the organization. **Assessment** *Determine if*: *(i) the organization develops and documents written policy and procedures for identity proofing and enrollment (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	FIPS 201-1 2.2 PIV Identity Proofing and Registration Requirements
	DO-3	The organization has a written policy and procedures for issuance which are signed off by the head of the organization. **Assessment** *Determine if*: *(i) the organization develops and documents a written policy and procedures for issuance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	FIPS 201-1 2.3 PIV Issuance and Maintenance Requirements
	DO-4	The organization has a written policy and procedures describing the conditions for PIV Card renewal which are signed off by the head of the organization. **Assessment** *Determine if*: *(i) the organization develops and documents a written policy and procedures for card renewal (review);*	FIPS 201-1 5.3.2.1 PIV Card Renewal

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review); *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	
	DO-5	The organization has a written policy and procedures describing the conditions for PIV Card termination which are signed off by the head of the organization. **Assessment** *Determine if*: *(i) the organization develops and documents a written policy and procedures for PIV Card termination (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy as required (review, interview).*	FIPS 201-1 5.3.2.4 PIV Card Termination
	DO-6	The organization has a written policy and procedures describing the conditions for PIV Card re-issuance which are signed off by the head of the organization. **Assessment** *Determine if*: *(i) the organization develops and documents a written policy and procedures for re-issuance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head of the organization (review);* *(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	FIPS 201-1 5.3.2.2 PIV Card Reissuance
	DO-7	In cases where a PIV Card is not required, such as temporary employees and contractors employed for less than 6 months and visitors, the organization has a written policy and procedures describing the conditions for temporary badges. **Assessment** *Determine if*: *(i) the organization develops and documents a written policy and procedures for the issuance of temporary badges (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization periodically reviews and updates the policy and procedures as required (review, interview).*	OMB Memorandum 05-24

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Assignment of Roles and Responsibilities	RR-1	The organization has appointed the role of Senior Authorizing Official (SAO). **Assessment** *Determine if*: *(i) the organization has defined the role of Senior Authorizing Official and its responsibilities according to the requirements of SP 800-79-1 (interview);* *(ii) the organization has documented the role of Senior Authorizing Official in the operations plan (review);* *(iii) the organization has appointed someone to the role of Senior Authorizing Official (interview).*	SP 800-79-1, Section 2.6 – Roles and Responsibilities
	RR-2	The organization has appointed the role of Designated Accreditation Authority (DAA). **Assessment** *Determine if*: *(i) the organization has defined the role of Designated Accreditation Authority and its responsibilities according to the requirements of SP 800-79-1 (interview);* *(ii) the organization has documented the role of Designated Accreditation Authority in the operations plan (review);* *(iii) the organization has appointed someone to the role of Senior Authorizing Official (interview).*	SP 800-79-1, Section 2.6 – Roles and Responsibilities
	RR-3	The organization has appointed the role of Organization Identity Management Official. **Assessment** *Determine if*: *(i) the organization has defined the role of Organization Identity Management Official and its responsibilities according to the requirements of SP 800-79-1 (interview);* *(ii) the organization has documented the role of Organization Identity Management Official in the operations plan (review);* *(iii) the organization has appointed someone to the role of Organization Identity Management Official (interview).*	SP 800-79-1, Section 2.6 – Roles and Responsibilities
	RR-4	The organization has appointed the role of Assessor. **Assessment** *Determine if*: *(i) the organization has defined the role of Assessor and its responsibilities according to the requirements of SP 800-79-1 (interview);* *(ii) the organization has documented the role of Assessor in the operations plan (review);* *(iii) the organization has appointed someone to the role of Assessor (interview);* *(iv) the Assessor is independent of, and organizationally separate from, the persons and office(s) directly responsible for the day-to-day operation of the organization (review, interview).*	SP 800-79-1, Section 2.6 – Roles and Responsibilities
	RR-5	The organization has appointed the role of Privacy Official (PO). **Assessment** *Determine if*: *(i) the organization has defined the role of Privacy Official*	SP 800-79-1, Section 2.6 – Roles and Responsibilities

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		and its responsibilities according to the requirements of SP 800-79-1 (interview); *(ii) the organization has documented the role of Privacy Official in the operations plan (review);* *(iii) the organization has appointed someone to the role of Privacy Official (interview);* *(iv) the Privacy Official does not have any other roles in the PCI (review, interview).*	
	RR-6	The PCI Facility employs processes which adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV Card without the cooperation of another authorized person. **Assessment** *Determine if*: *(i) the PCI facility documents in standard operating procedures the principle of separation of duties (review);* *(ii) the PCI facility's processes demonstrate adherence to the principle of separation of duties (interview, observe).*	FIPS 201-1, Section 5.2 – PIV Identity Proofing and Registration
Facility and Personnel Readiness	**Facility**		
	FP-1	The PCI Facility is housed within a federally owned or leased building that meets or exceeds current Interagency Security Committee (ISC) security standards for Federal buildings. [review, observe] **Assessment** *Determine if:* *(i) management for the building in which the PCI Facility is located has documentation showing that the building has gone through a vulnerability assessment and meets ISC security standards for Federal buildings (review).*	Commonly accepted security readiness measures
	FP-2	The PCIF Manager has a System Security Plan, a Configuration/Change Management Plan and a Contingency Plan for the operations of all the IT processing, storage and communication resources in the PCI facility. **Assessment** *Determine if*: *(i) the PCI Facility has a System Security Plan, a Configuration/Change Management and a Contingency Plan and they contain information specific enough to be utilized in the operations of the PCI Facility (review).*	Commonly accepted security readiness measures
	Equipment		
	FP-3	The PCI Facility provides mechanisms (such as VPN routers) to protect the confidentiality and integrity of information transmitted between information systems and their individual components such as IDMS. **Assessment** *Determine if*: *(i) the PCI Facility provides mechanisms (such as VPN routers) to protect the confidentiality and integrity of information transmitted between information systems and their individual components such as IDMS (interview);* *(ii) the mechanisms (such as VPN routers) to protect the confidentiality and integrity of information transmitted between information systems and their individual components such as IDMS are documented in the system architecture diagrams / descriptions (review).*	Commonly accepted security readiness measures

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
	FP-4	Enrollment/identity proofing and card activation/issuance workstations are situated in an enclosed area (wall or partition) to provide privacy for applicant or card holder. **Assessment** *Determine if*: *(i) PCI Facility workstations are situated in an enclosed area (wall or partition) such that other individuals cannot see an applicant or card holder's personal information (observe).*	Commonly accepted security readiness measures
	Key Personnel		
	FP-5	All operators who perform roles within a PCI Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed access to information systems only when authenticated through a PIV Card. **Assessment** *Determine if*: *(i) The requirement that all operators who perform roles within a PCI Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed access to information systems only when authenticated through a PIV Card has been documented in the PCI Facility's standard operating procedures (review);* *(ii) Operators are knowledgeable of the requirement that individuals who perform roles within a PCI Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed access to information systems only when authenticated through a PIV Card (interview);* *(iii) Operators use PIV cards to access information systems in the course of performing their roles in the areas of enrollment/ identity proofing or card activation/issuance access.*	Commonly accepted security readiness measures
	Operations/Maintenance Personnel		
	FP-6	All pre-personalized or personalized smart card stock received from card production facilities are received by a designated receiving official who ensures that they are stored securely in the PCI Facility. **Assessment** *Determine if*: *(i) a receiving official has been designated to ensure that smart card stock is received and stored securely in the PCI Facility (interview);* *(ii) procedures for receiving and storing smart card stock are documented in the PCI Facility's standard operating procedures (review);* *(iii) the receiving official is knowledgeable of the procedures on how to receive and store smart card stock (interview).*	Commonly accepted security readiness measures
	Other		
	FP-7	The organization maintains a current list of designated point of contacts and alternate point of contacts for all PCIFs used by the organization for enrollment/identity proofing and card activation/issuance. **Assessment** *Determine if*: *(i) the organization maintains a current list of designated point of contacts and alternate point of contacts for all PCIFs used by the organization for enrollment/identity proofing and card activation/issuance (review).*	Commonly accepted security readiness measures

PAT = Organizational Preparedness			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
	FP-8	If the organization is utilizing the services of an external service provider, its Service Level Agreement (SLA) with the provider covers the PCI controls FP-2 through FP-6. **Assessment** *Determine if*: *(i) If the organization is utilizing the services of an external service provider, its Service Level Agreement (SLA) with the provider covers the PCI controls FP-2 through FP-6 (review).*	Commonly accepted security readiness measures

PAT = Security Management & Data Protection			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Protection of Stored and Transmitted Data	SY-1	The PCI information systems that contain information in identifiable form are handled in compliance with federal laws and policies including the Privacy Act of 1974. **Assessment** *Determine if*: *(i) the PCI Facility does not disclose any record which is contained in the system of records to any person, or to another organization unless written consent has been given by the individual to whom the record pertains unless one of the exceptions for disclosure in the Privacy Act are met (review, interview);* *(ii) individuals are permitted to gain access to their personal record and the information is provided in a form comprehensible to them (review, interview);* *(iii) individuals are able to request amendments to records pertaining to them, corrections are made promptly and if not, the individual is provided with a reason for the refusal and is able to request a review of the refusal (review, interview);* *(iv) the organization notifies an individual when their record is made available to any person under a compulsory legal process when such a process becomes a matter of public record (review, interview).*	FIPS 201-1 2.4 PIV Privacy Requirements
	SY-2	The information systems protect the integrity and confidentiality of transmitted information through the use of encryption or other alternate physical protection means. **Assessment** *Determine if*: *(i) the integrity of transmitted information is protected by encryption or other alternate physical protection means (interview, test)* *(ii) the confidentiality of transmitted information is protected by encryption or other alternate physical protection means (interview, test)*	FIPS 201-1 2.4 PIV Privacy Requirements

PAT = Security Management & Data Protection			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Enforcement of	PR-1	The organization has developed and posted at the PCI Facility in	OMB Memorandum 05-24

PAT = Security Management & Data Protection			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Privacy Requirements		multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies. **Assessment** *Determine if*: *(i) the PCI Facility has posted privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies (interview, observe).*	
	PR-2	The organization has conducted a Privacy Impact Assessment of their PCI information system (s), constituent with Section 208 of the E-Government Act of 2002 and at a minimum, addresses guidance found in Appendix E of OMB Memorandum 06-06. **Assessment** *Determine if:* *(i) the organization has conducted a Privacy Impact Assessment of their PCI information system (s) which addresses guidance found in Appendix E of OMB Memorandum 06-06 (review);* *(ii) the organization has submitted the Privacy Impact Assessment of their PCI information system (s) to OMB (interview).*	OMB Memorandum 05-24
	PR-3	The organization's employee and contractor identification systems of records notices (SORN's) are updated to reflect any changes in the disclosure of information to other organizations consistent with the Privacy Act of 1974 and OMB Circular A-130, Appendix 1. **Assessment** *Determine if:* *(i) the organization updates SORN's to reflect changes in the disclosure of information (review, interview).*	OMB Memorandum 05-25
	PR-4	The applicant is notified of what information in identifiable form is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information. **Assessment** *Determine if:* *(i) the PCI Facility requires the PIV Card applicant to be notified before receiving a PIV Card which notifies them of what information in identifiable form is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (review, observe)*	FIPS 201-1, Section 2.4 – PIV Privacy Requirements
	PR-5	The PCI Facility employs technologies that allow for continuous auditing of compliance with privacy policies and practices. **Assessment** *Determine if:* *(i) the PCI Facility employs technologies that allow for the continuous auditing of compliance with privacy policies and practices. This could include the use of technology to*	FIPS 201-1, Section 2.4 – PIV Privacy Requirements

PAT = Security Management & Data Protection			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		monitor data access, data flows between information systems and the use of Individually Identifiable Information (interview, test).	
	PR-6	In the case of termination, any Individually Identifiable Information (IIF) that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies. **Assessment** *Determine if:* *(i) as a part of PIV Card termination, the organization disposes of IIF in accordance with its privacy and data retention policies (review, interview).*	FIPS 201-1, Section 5.3.2.4 – PIV Card Termination

Infrastructure Elements			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Deployed Products & Information Systems	DP-1	In order to be compliant with the provisions of OMB Circular A-130, App III, the PCI information system(s) are certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. **Assessment** *Determine if:* *(i) the organization has a letter showing the current accreditation decision of each information system used to support the PCI (review).*	FIPS 201-1, Appendix B.2 – Security Certification and Accreditation of IT System(s)
	DP-2	Every product utilized by a PCI facility must be on the GSA FIPS 201 Evaluation Lab's Approved Product List if it falls within one of the categories listed by that program. **Assessment** *Determine if:* *(i) for each product that falls within one of the categories listed within the APL, its make, model and version is compared against the APL (observe)*	OMB Memorandum 05-24
	DP-3	The organization has submitted the PIV Card to GSA for testing and they have approved it. **Assessment** *Determine if:* *(i) the organization has a letter from the GSA showing their approval of the card (review).*	OMB Memorandum 07-06

PAT = Infrastructure Elements			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Implementation of Credentialing Infrastructures	CI-1	For legacy Public Key Infrastructures (PKI's), the organization's CA shall be cross-certified with the Federal Bridge (FBCA) at Medium-HW or High Assurance Level. **Assessment**	FIPS 201-1, Section 5.4.4 – Migration from Legacy PKIrs

PAT = Infrastructure Elements			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		Determine if: *(i) the PKI is listed on the FBCA's website as being cross-certified (review).*	
	CI-2	For non-legacy PKI's, the CA that issues certificates to support PIV Card authentication participates in the hierarchical PKI for the Common Policy managed by the Federal PKI. **Assessment** *Determine if:* *(i) the PKI is listed on the FPKI PA's website as being a shared service provider (review).*	FIPS 201-1, Section 5.4.1 – Architecture
	CI-3	When cards are personalized, card management keys are set to be specific to each PIV Card. That is, each PIV Card shall contain a unique card management key. **Assessment** *Determine if:* *(i) the CMS Vendor's documentation shows the use of unique card management keys (review);* *(ii) the OIMO indicates that card management keys are unique. (interview).*	FIPS 201-1, Section 4.1.6.2 – Activation by Card Management System
	CI-4	Fingerprint images retained by organizations shall be formatted according to SP 800-76-1. **Assessment** *Determine if:* *(i) the fingerprint images are formatted according to Table 4 in SP 800-76-1 and INCITS 381 (test).*	SP 800-76-1, Section 3.4 – Fingerprint Template Specifications
	CI-5	Facial images collected during enrollment/identity proofing are formatted such that they conform to SP 800-76-1. **Assessment** *Determine if:* *(i) the facial images are formatted according to Table 6 in SP 800-76-1 and INCITS 385 (test).*	SP 800-76-1, Section 5.2 – Acquisition and Format
	CI-6	The fingerprint templates stored on the PIV Card are prepared from images of the primary and secondary fingers. **Assessment** *Determine if:* *(i) the fingerprint templates are prepared from images of the primary and secondary fingers (test).*	SP 800-76-1, Section 3.4.1 – Source Images
	CI-7	Logical data elements loaded on the PIV Card conform to SP 800-85B – PIV Data Model Conformance Guidelines **Assessment** *Determine if:* *(i) the PIV Card passes the testing with the SP 800-85B test tool (test).*	OMB Memorandum 07-06

PAT = Processes

Accreditation Focus Area	Identifier	PCI Control	Source
Sponsorship Process	SN-1	A request is created in order to issue a PIV Card. **Assessment** *Determine if:* *(i) the process for making a request is documented (review);* *(ii) A PIV Request is created in order to issue a PIV Card (observe).*	FIPS 201-1 2.1 Control Objectives
	SN-2	The PCI Facility collects personal information using only forms approved by OMB under the Paperwork Reduction Act of 1995. **Assessment** *Determine if*: *(i) forms used to collect personal information have been approved by OMB (review, observe).*	OMB Memorandum 07-06

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Enrollment / Identity Proofing Process	EI-1	The PCI Facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the Applicant. **Assessment** *Determine if:* *(i) the PCI Facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the Applicant (interview, observe);* *(ii) the PCI Facility has materials used to train enrollment/identity proofing officials on how to verify the authenticity of the source documents (review).*	FIPS 201-1 2.1 Control Objectives
	EI-2	The PCI Facility requires the Applicant to appear in-person at least once before the issuance of a PIV Card. **Assessment** *Determine if:* *(i) the requirement that an applicant appear in-person at least once before the issuance of a PIV Card is documented (review);* *(ii) the Applicant appears in-person at least once before the issuance of a PIV Card (observe).*	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements
	EI-3	Two identity source documents are checked in accordance with the requirements of Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. **Assessment** *Determine if:* *(i) the requirement to check two identity source documents in accordance with the requirements of Form I-9 is documented (review);* *(ii) two identity source documents are checked in accordance with the requirements of Form I-9 during enrollment/identity proofing (observe).*	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements
	EI-4	One of the identity source documents used to verify the claimed identity of the Applicant is a valid Federal or State government issued photo identification. **Assessment** *Determine if:*	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(i) the requirement that one of the identity source documents is a valid Federal of State government issued photo ID is documented (review); *(ii) one of the identity source documents used to verify the claimed identity of the Applicant is a valid Federal or State government issued photo identification (observe).*	
	EI-5	The PCI Facility performs the entire identity proofing and enrollment/identity proofing process prior to re-issuing a PIV Card. **Assessment** *Determine if:* *(i) the requirement to perform the entire identity proofing and enrollment process prior to re-issuing a PIV Card is documented (review);* *(ii) the PCI Facility performs the entire identity proofing and enrollment process prior to re-issuing a PIV Card (observe).*	FIPS 201-1, Section 5.3.2.2 PIV Card Reissuance
	EI-6	A new facial image is collected at the time of renewal. **Assessment** *Determine if:* *(i) the requirement to capture a new facial image is documented within the renewal process (review);* *(ii) a new facial image is collected at the time of renewal (observe).*	FIPS 201-1, Section 4.4 – Biometric Data Specifications
	EI-7	The biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the enrollment/identity proofing process. **Assessment** *Determine if:* *(i) the requirement to capture biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during enrollment/identity proofing process is documented (review);* *(ii) The biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the enrollment/identity proofing process (observe).*	FIPS 201-1, Section 5.2 – PIV Identity Proofing and Registration Requirement
	EI-8	A cardholder waits until six weeks prior to the expiration of a valid PIV Card before applying for renewal. **Assessment** *Determine if:* *(i) the requirement that a cardholder must wait until six weeks prior to the expiration of a valid PIV Card before applying for renewal is documented (review);* *(ii) a cardholder waits until six weeks prior to the expiration of a valid PIV Card before applying for renewal (interview).*	FIPS 201-1, Section 5.3.2.1 – PIV Card Renewal
	EI-9	The PCI Facility captures the Applicant's fingerprints in accordance to any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card. **Assessment** *(i) the PCI Facility captures the Applicant's fingerprints in accordance to any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card*	SP 800-76-1, Section 3.3 – Fingerprint Image Acquisition

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(observe).	
	EI-10	The PCI Facility has an attending official present at the time of fingerprint capture. **Assessment** *Determine if:* *(i) the requirement that the PCI Facility has an attending official present at the time of fingerprint capture is documented (review);* *(ii) the PCI Facility has an attending official present at the time of fingerprint capture (observe).*	SP 800-76-1, Section 3.3 – Fingerprint Image Acquisition
	EI-11	The PCI Facility acquires fingerprint images in accordance with Table 2 in 800-76-1. **Assessment** *Determine if:* *(i) fingers are inspected for the absence of foreign materials (observe);* *(ii) scanner and card surfaces are clean (observe);* *(iii) the presentation of fingers for a plain live scan, rolled live scan, and rolled ink card are based on procedures in Table 1 (observe);* *(iv) multi-finger plain impression images are properly segmented into single finger images (observe).*	SP 800-76-1, Section 3.3 – Fingerprint Image Acquisition
	EI-12	The PCI Facility captures the 10 fingerprints of the Applicant. In the case where less than ten fingers are collected, the missing fingers are labeled before transmitting to the FBI. **Assessment** *Determine if:* *(i) the requirement that the PCI Facility captures the 10 fingerprints of the Applicant and labels any missing fingers is documented (review);* *(ii) the PCI Facility captures the 10 fingerprints of the Applicant and labels any missing fingers (observe).*	SP 800-76-1, 3.3 Fingerprint image acquisition

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Adjudication Process	AD-1	The organization conducts a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management (OPM) or National Security community investigation for each Applicant for whom a successfully adjudicated NACI cannot be referenced on file. **Assessment** *Determine if:* *(i) the requirement that the organization conduct a National*	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(ii) the organization conducts a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management (OPM) or National Security community investigation for each Applicant for whom a successfully adjudicated NACI cannot be referenced on file (interview).	
	AD-2	The organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the PIV Card is issued. **Assessment** *Determine if:* *(i) the requirement that the organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the PIV Card is issued is documented (review);* *(ii) the organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the PIV Card is issued (interview).*	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Card Production Process	CP-1	The PIV Card implements security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. **Assessment** *Determine if:* *(i) the PIV Card contains at least one security feature. Examples of these security features include the following: (i) Optical varying structures, (ii) Optical varying inks, (iii) Laser etching and engraving, (iv) Holograms, (v) Holographic images, (vi) Watermarks (interview, observe*).	FIPS 201-1, Section 4.1.2 – Tamper Proofing and Resistance
	CP-2	The PIV Card is not embossed. **Assessment** *Determine if:* *(i) the PIV Card is not embossed (review, observe)*	FIPS 201-1, Section 4.1.3 – Physical Characteristics and Durability
	CP-3	Decals are not adhered to the PIV Card. **Assessment** *Determine if:* *(i) decals are not adhered to the PIV Card (review, observe).*	FIPS 201-1, Section 4.1.3 – Physical Characteristics and Durability
	CP-4	If organizations choose to punch an opening in the card body to enable the card to be worn on a lanyard, all such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity is not adversely impacted. **Assessment** *Determine if:*	FIPS 201-1, Section 4.1.3 – Physical Characteristics and Durability

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(i) the integrity of a PIV Card is not affected by a punched opening (test).	

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Card Activation / Issuance Process	AI-1	The personalized PIV Card complies with all the mandatory items on the front of the PIV Card. **Assessment** *Determine if:* *(i) the PIV Card meets specific requirements in FIPS 201-1 for (i) photograph; (ii) name; (iii) employee; affiliation; (iv) and expiration date (observe).*	FIPS 201-1, Section 4.1.4.1 – Mandatory Items on the Front of the PIV Card
	AI-2	The personalized PIV Card complies with all the mandatory items on the back of the PIV Card. **Assessment** *Determine if:* *(i) the PIV Card meets specific requirements in FIPS 201-1 for (i) organization card serial number; (ii) and issuer identification (observe).*	FIPS 201-1, Section 4.1.4.2 – Mandatory Items on the Back of the Card
	AI-3	If one or more optional items are printed on the front of the PIV Card, they comply with the requirements for the optional items on the front on the PIV Card. **Assessment** *Determine if:* *(i) the PIV Card meets specific requirements in FIPS 201-1 if it includes optional items on the front of the card such as (i) signature; (ii) organization specific text area; (iii) rank; (iv) portable data file; (v) header; (vi) organization seal; (vii) footer; (viii) issue date; (ix) color-coding employee affiliation; (x) photo border for employee affiliation; (xi) organization specific data (observe).*	FIPS 201-1, Section 4.1.4.3 – Optional Items on the Front of the Card
	AI-4	If one or more optional items are printed on the back of the PIV Card, they comply with the requirements for the optional items on the back on the PIV Card. **Assessment** *Determine if:* *(i) the PIV Card meets specific requirements in FIPS 201-1 if it includes optional items on the front of the card such as (i) magnetic stripe; (ii) return to; (iii) physical characteristics of cardholder; (iv) additional language for emergency responder officials; (v) standard Section 499, Title 18 language; (vi) linear 3 of 9 bar code; (vii) organization specific text (zones 9 & 10) (observe).*	FIPS 201-1, Section 4.1.4.4 – Optional Items on the Back of the Card

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
	AI-5	The PIV Card includes mechanisms to limit the number of PIN guesses an adversary can attempt if a card is lost or stolen. **Assessment** *Determine if:* *(i) the PIV Card limits the number of incorrect PIN guesses (test).*	FIPS 201-1, Section 4.1.6.1 – Activation by Cardholder
	AI-6	The PIV Card is valid for no more than five years. **Assessment** *Determine if:* *(i) the expiration date printed on the PIV Card is no more than five years from the issuance date (observe, test).* *(ii) the expiration date printed in the CHUID*	FIPS 201-1, Section 5.3.2.1 – PIV Card Renewal
	AI-7	The PCI Facility performs a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record before releasing the PIV Card to the applicant. **Assessment** *Determine if:* *(i) the requirement that the issuer performs a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record is documented (review);* *(ii) the issuer performs a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record (observe).*	FIPS 201-1, Section 5.3.1 – PIV Card Issuance
	AI-8	The PCI Facility performs a 1:1 biometric match of the PIV Card holder against the biometric included in the PIV Card or in the PIV enrollment record prior to renewal. **Assessment** *Determine if:* *(i) the requirement that the PCI Facility performs a 1:1 biometric match of the PIV Card holder against the biometric included in the PIV Card or in the PIV enrollment record prior to renewal is documented (review);* *(ii) the PCI Facility performs a 1:1 biometric match of the PIV Card holder against the biometric included in the PIV Card or in the PIV enrollment record prior to renewal (observe).*	FIPS 201-1, Section 5.3.2.1 – PIV Card Renewal
	AI-9	The PCI Facility advises applicants that the PIN on the PIV Card should not be easily-guess-able or otherwise individually-identifiable in nature. **Assessment** *Determine if:* *(i) the requirement that the PCI Facility advises applicants that the PIN on the PIV Card should not be easily-guess-able or otherwise individually-identifiable in nature is documented (review);* *(ii) the PCI Facility advises applicants that the PIN on the PIV Card should not be easily-guess-able or otherwise individually-identifiable in nature (observe).*	FIPS 201-1, Section 4.1.6.1 Activation by Cardholder
	AI-10	Identity cards issued to individuals without a completed NACI or equivalent are electronically distinguishable from identity cards issued to individuals who have a completed investigation.	FIPS 201-1, Section 2.2 – PIV Identity Proofing and Registration Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		Assessment *Determine if:* *(i) the PCI Facility has procedures for how to update the NACI interim indicator extension for identity cards issued to individuals without a completed NACI or equivalent (review, interview);* *(ii) for individuals without a completed NACI or equivalent, the NACI interim indicator is set to true (test);* *(iii) for individuals with a completed NACI or equivalent, the NACI interim indicator is set to false (test).*	
	AI-11	After PIN reset on the PIV Card, the PCI Facility performs a 1:1 biometric match of the PIV Card holder against the biometric included in the PIV Card or in the PIV enrollment record before releasing the PIV Card. **Assessment** *Determine if:* *(i) the requirement that after PIN reset on the PIV Card, the PCI Facility performs a 1:1 biometric match of the PIV Card holder against the biometric included in the PIV Card or in the PIV enrollment record before releasing the PIV Card is documented (review);* *(ii) after PIN reset on the PIV Card, the PCI Facility performs a 1:1 biometric match of the PIV Card Holder against the biometric included in the PIV Card or in the PIV enrollment record before releasing the PIV Card (observe).*	FIPS 201-1, Section 5.3.2.3 – PIV Card PIN Reset
	AI-12	The PCI Facility issues an electro-magnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential. **Assessment** *Determine if*: *(i) the requirement that the PCI Facility issue an electro-magnetically opaque sleeve with every PIV Card is documented (review);* *(ii) the PCI Facility issues an electro-magnetically opaque sleeve with every PIV Card (interview, observe).*	FIPS 201-1, Section 2.4 – Privacy Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
Maintenance Process	MP-1	The PIV FASC-N is not modified post-issuance. **Assessment** *Determine if:* *(i) the PIV FASC-N is not modified post-issuance (review, interview).*	FIPS 201-1, Section 4.2 – Cardholder Unique Identifier
	MP-2	In the case of a renewal, re-issuance and termination, the PIV Card is collected and destroyed whenever possible. **Assessment** *Determine if:* *(i) the requirement that in the case of a renewal, re-issuance and termination, the PIV Card is collected and destroyed whenever possible is documented (review);*	FIPS 201-1, Section 2.3 – PIV Issuance and Maintenance Requirements

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		(ii) in the case of a renewal, re-issuance and termination, the PIV Card is collected and destroyed whenever possible (interview).	
	MP-3	Normal operational procedures must be in place to ensure proper card revocation during PIV Card re-issuance and termination: (i) The PIV Card itself is revoked; (ii) Databases containing Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status; (iii); and (iv) Online Certificate Status Protocol (OCSP) responders are updated so that queries with respect to certificates on the PIV Card are answered appropriately. **Assessment** *Determine if:* *(i) during card revocation the PIV Card is revoked (review, interview);* *(ii) databases containing Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status (interview);* *(iii) the CA is informed and the certificates on the PIV Card are revoked (test);* *(iv) online Certificate Status Protocol (OCSP) responders are updated (test).*	FIPS 201-1 Section 5.3.2.4 PIV Card Termination
	MP-4	If the PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification. **Assessment** *Determine if:* *(i) the requirement that PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification is documented (review);* *(ii) if the PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification (observe).*	FIPS 201-1, Section 5.3.2.2 – PIV Card Reissuance
	MP-5	Upon PIV Card termination, the organization enforces a standard methodology of updating systems of records to indicate employee termination and this status is replicated throughout relying systems used for physical and logical access to organization facilities and resources. **Assessment** *Determine if:* *(i) the PCI Facility has documented its procedures for updating information systems to indicate employee termination (review);* *(ii) the PCI Facility updates information systems to indicate employee termination (interview).*	FIPS 201-1 5.3.2 PIV Card Maintenance
	MP-6	The organization posts a quarterly report, stating the number of PIV Cards issued to date, to the organization's website and the link is emailed to OMB. **Assessment** *Determine if:* *(i) the organization develops and post a quarterly report to the organization's website according to the requirements of the attachment to OMB memorandum 07-06 (review);* *(ii) the organization sends the link to the report to OMB on a*	OMB Memorandum 07-06

PAT = Processes			
Accreditation Focus Area	**Identifier**	**PCI Control**	**Source**
		quarterly basis (review, interview).	
	MP-7	The organization has completed a life-cycle walk-through at one-year intervals since the last accreditation date and the results are documented in a report to the DAA. **Assessment** *Determine if*: *(i) the organization has completed a life-cycle walk-through to cover sponsorship, enrollment/identity proofing, card production, card activation/issuance and maintenance processes (interview);* *(ii) a life-cycle walk-through has been completed at one year intervals since the last accreditation date (interview);* *(iii) the results of the PCI life-cycle walk-through have been documented and reviewed by the DAA (review, interview).*	SP 800-79-1 Section 5.4 - Monitoring Phase

APPENDIX H: ASSESSMENT AND ACCREDITATION TASKS FOR PIV CARD ISSUERS (PCI'S)

Phases, Tasks, and Sub-tasks	Person(s) Responsible
Initiation Phase	
Task 1: Preparation	
Subtask 1.1: Confirm that the PCI and its operations have been fully described and documented in the PCI's operations plan.	OIMO
Subtask 1.2: Confirm that the PCI's services and/or information systems have not been categorized as National Security.	OIMO
Subtask 1.3: Confirm that the PCI has documented in the operations plan its processes for the major functional areas including enrollment/identity proofing, card production, card activation/issuance and maintenance.	OIMO
Subtask 1.4: Confirm that processes conducted by the PCI Facility are in accordance with the policies and procedures specified in the PCI operations plan and are documented in Standard Operating Procedures.	OIMO, PCIF Manager
Task 2: Resource Identification	
Subtask 2.1: Identify the SAO, DAA, PO, Assessor(s), and other organization officials such as enrollment/identity proofing and card activation/issuance personnel who can provide information to the Assessor. Notify these individuals of the upcoming assessment and inform them of the need for their participation during the process.	OIMO
Subtask 2.2: Determine the accreditation boundary.	OIMO, DAA
Subtask 2.3: Determine the resources and the time needed for the accreditation of the PCI and prepare a plan of execution.	OIMO, DAA
Task 3: Operations Plan Analysis and Acceptance	
Subtask 3.1: Review the list of required PCI controls documented in the organization's operation plan to confirm that they have been implemented properly.	OIMO, DAA

Phases, Tasks, and Sub-tasks		Person(s) Responsible
Subtask 3.2:	Analyze the PCI operations plan to determine if there are deficiencies in satisfying all the policies, procedures, and other requirements in FIPS 201-1 and that could result in a DATO being issued. After discussing the discovered deficiencies in the documentation and operations plan with the OIMO, the organization may still want to continue with the assessment. If so, the DAA must authorize the continuation of the assessment.	OIMO, DAA
Subtask 3.3:	Verify that the PCI operations plan is acceptable.	DAA

Assessment Phase

Task 4: PCI Control Assessment		
Subtask 4.1:	For each PCI control review the suggested and selected assessment methods in preparation for the assessment.	Assessor
Subtask 4.2:	Assemble all documentation and supporting materials necessary for the assessment of the PCI; if these documents include previous assessments, review the findings and determine if they are applicable to the current assessment.	OIMO, Assessor
Subtask 4.3:	Assess the required PCI controls using the selected assessment procedures.	Assessor
Subtask 4.4:	Prepare the assessment report.	Assessor
Task 5: Assessment Documentation		
Subtask 5.1:	Provide the OIMO with the assessment report.	Assessor
Subtask 5.2:	Revise the PCI operations plan (if necessary) and implement its new provisions.	OIMO
Subtask 5.3:	Prepare the CAP.	OIMO
Subtask 5.4:	Assemble the accreditation package and submit to DAA.	Assessor, OIMO

Phases, Tasks, and Sub-tasks		Person(s) Responsible
Accreditation Phase		
Task 6: Accreditation Decision		
Subtask 6.1:	Determine the risk to the organization's operations, assets, or individuals based on the PCI's deficiencies and the CAP and perform a final assessment review.	DAA
Subtask 6.2:	Determine if the risk to the organization's operations, assets, or potentially affected individuals is acceptable, that the PCI controls have been adequately assessed and prepare the final accreditation decision letter.	DAA
Task 7: Accreditation Documentation		
Subtask 7.1:	Provide copies of the final accreditation package including the accreditation decision letter, in either paper or electronic form, to the OIMO and any other organization officials having interests, roles, or responsibilities in the PCI.	DAA
Subtask 7.2:	Update the PCI's operations plan.	OIMO
Monitoring Phase		
Task 8: Operations Plan Update		
Subtask 8.1:	Document all relevant changes in the PCI within the operations plan.	OIMO
Subtask 8.2:	Analyze the proposed or actual changes to the PCI and determine the impact of such changes.	OIMO
Task 9: Life-cycle Walk-through		
Subtask 9.1:	An organization official observes all the processes involved in getting a PIV Card, including those going from sponsorship to maintenance. The official should observe each process and compare its controls against the applicable list of required PCI controls. If a PCI has several facilities, this process should be repeated using randomly selected of PCIFs.	OIMO, organization official
Subtask 9.2:	The results of the life-cycle walk-through are summarized in a report to the DAA. Deficiencies must be highlighted along with corrective actions that must be done to correct the deficiencies.	OIMO, DAA